STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 4971
2 februari
2016

Beleidsregels cameratoezicht, College bescherming persoonsgegevens

Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens

Samenvatting

Deze beleidsregels Cameratoezicht vervangen de publicatie *'Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde'* (2004) van het College bescherming persoonsgegevens (CBP), tegenwoordig de Autoriteit Persoonsgegevens. Diverse ontwikkelingen, zowel op het gebied van wetgeving als op het gebied van de technologie, waren aanleiding voor deze nieuwe publicatie.

De beleidsregels vormen een uitwerking van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens die relevant zijn voor cameratoezicht door private of publieke organisaties *ter beveiliging van personen en goederen* en door gemeenten ter *handhaving van de openbare orde*. Ook wordt ingegaan op de inzet van nieuwe technologieën bij cameratoezicht, zoals drones, dashcams en andere slimme camera's.

Aangezien de bepalingen van de Wet bescherming persoonsgegevens (Wbp) *algemeen* van aard zijn, kan de uitwerking van die bepalingen in deze beleidsregels ook van toepassing zijn op verwerkingen van ander beeldmateriaal, zoals foto's, en voor andere doeleinden, zoals camera*observatie*, die ook onder het wettelijke regime van de Wbp vallen.

De beleidsregels dienen in eerste instantie als leidraad voor organisaties die gebruik (willen) maken van cameratoezicht en als uitgangspunt voor de Autoriteit Persoonsgegevens bij haar toezichthoudende taak. Daarnaast kunnen ze ook voor ontwikkelaars en leveranciers van (slimme) digitale camerasystemen als leidraad dienen bij de ontwikkeling van (nieuwe) technologie waarbij sprake is van de verwerking van beeldmateriaal.

Inleiding

Organisaties zetten steeds vaker cameratoezicht in. Hierbij verwerken zij vaak persoonsgegevens. Bovendien worden de technische mogelijkheden van camera's steeds geavanceerder. Zo worden camera's bijvoorbeeld gekoppeld aan drones[1] en worden ze steeds 'slimmer' gemaakt, waardoor ze steeds meer informatie kunnen genereren.

De toename in het gebruik van cameratoezicht en de voortschrijdende technologie maakt dat er bij bedrijven en overheden een groeiende behoefte bestaat aan inzicht in de wettelijke mogelijkheden om cameratoezicht toe te passen. De Autoriteit Persoonsgegevens brengt daarom deze beleidsregels cameratoezicht uit.

De beleidsregels zijn ten eerste toegespitst op cameratoezicht door (private of publieke) organisaties ter beveiliging van personen en goederen, waarop de Wet bescherming persoonsgegevens (Wbp) van toepassing is. Ten tweede gaan zij in op cameratoezicht door gemeenten ter handhaving van de openbare orde, waarop artikel 151c Gemeentewet van toepassing is. Met 'cameratoezicht' wordt in deze beleidsregels de bewaking met camera's bedoeld. Dat neemt niet weg dat de bepalingen van de Wbp algemeen van aard zijn, zodat de uitwerking van die bepalingen in deze beleidsregels ook van toepassing kan zijn op verwerkingen van ander beeldmateriaal, zoals foto's, en voor andere doeleinden, zoals camera*observatie*, die ook onder het wettelijke regime van de Wbp vallen. Met 'cameraobservatie' wordt bedoeld het waarnemen met camera's, anders dan bewaking.

Bij de uitwerking van artikel 151c Gemeentewet in deze beleidsregels komen de rol en verantwoordelijkheden van de politie met betrekking tot cameratoezicht in het kader van de handhaving van de openbare orde aan bod. De beleidsregels gaan echter *niet* specifiek in op cameratoezicht in het kader van de algemene politietaak in de zin van artikel 3 Politiewet 2012, noch op de opsporing en vervolging van strafbare feiten. Daarentegen bevat hoofdstuk 1 van de beleidsregels wel algemene uitgangspunten die gelden wanneer persoonsgegevens worden verwerkt door middel van een camera. Deze uitgangspunten gelden in het algemeen, dus in principe ook wanneer cameratoezicht

[1] Een drone is een onbemand luchtvaartuig. Zie over het onderwerp drones Hoofdstuk 5.

plaatsvindt in het kader van de algemene politietaak of in het kader van opsporing en vervolging van strafbare feiten.

De beleidsregels dienen als leidraad bij zowel de afweging die organisaties dienen te maken alvorens zij tot cameratoezicht overgaan, als bij de maatregelen die zij vervolgens moeten treffen ter bescherming van de persoonsgegevens van de betrokkenen. Hoewel ontwikkelaars en leveranciers van camerasystemen meestal niet verantwoordelijk zijn voor de verwerking van persoonsgegevens door middel van camera's, kunnen de beleidsregels ook voor hen als leidraad dienen om al in de ontwikkelings- en leveringsfase van deze systemen rekening te houden met de bescherming van persoonsgegevens. Voor de Autoriteit Persoonsgegevens ten slotte dienen deze beleidsregels bovendien als uitgangspunt bij het onderzoeken en beoordelen van de inzet van cameratoezicht en bij het toepassen van handhavende maatregelen.

De beleidsregels beginnen met meer algemene uitgangspunten en worden daarna steeds specifieker. Zo bevat hoofdstuk 1 de algemene uitgangspunten die meestal gelden wanneer persoonsgegevens worden verwerkt door middel van een camera. Hoofdstuk 2 en 3 bevatten een uitwerking van belangrijke bepalingen uit de Wbp respectievelijk artikel 151c Gemeentewet j° de Wet politiegegevens (Wpg) ten aanzien van cameratoezicht. Hoofdstuk 4 gaat in op situaties waarin private organisaties delen van openbare plaatsen filmen en waarin private organisaties en gemeenten gezamenlijk zowel private goederen als openbare plaatsen filmen. In hoofdstuk 5 komt cameratoezicht door middel van drones, dashcams en (andere) slimme camera's aan bod. De beleidsregels worden met hoofdstuk 6 afgesloten, waarin de rechten van betrokkenen en de rol van de Autoriteit Persoonsgegevens kort worden beschreven. In de bijlagen zijn de belangrijkste wettelijke bepalingen opgenomen.

De beleidsregels vervangen de publicatie '*Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde*' van het College bescherming persoonsgegevens[2] uit november 2004. Deze eerdere publicatie gaat over cameratoezicht op de openbare orde (waarop thans artikel 151c Gemeentewet van toepassing is), terwijl deze beleidsregels ook betrekking hebben op cameratoezicht waarop de Wbp van toepassing is. De belangrijkste wijzigingen in de regelgeving die sindsdien hebben plaatsgevonden zijn de invoering van artikel 151c Gemeentewet en de invoering van de Wpg. Thans ligt de aanpassing van artikel 151c Gemeentewet in verband met de Wet flexibel cameratoezicht[3] bij de Eerste Kamer. Ten tijde van de publicatie van deze beleidsregels is deze wet nog niet in werking is getreden. Het is vanzelfsprekend aan de Eerste Kamer om te oordelen over het voornoemde wetsvoorstel; in deze beleidsregels is evenwel uitgegaan van de eventuele inwerkingtreding van de Wet flexibel cameratoezicht. De beleidsregels dienen immers over een langere tijdsperiode geldingskracht te hebben waarbij het streven is deze actueel te laten zijn.

In de beleidsregels worden relevante wettelijke bepalingen en jurisprudentie beschreven die van toepassing kunnen zijn op de verwerking van persoonsgegevens door middel van cameratoezicht. De genoemde wettelijke bepalingen en jurisprudentie zijn echter niet uitputtend. De voorbeelden in de beleidsregels dienen enkel ter illustratie en zijn ontdaan van andere relevante (juridische) omstandigheden. Een definitieve beoordeling over de rechtmatigheid van de verwerking van persoonsgegevens door middel van cameratoezicht kan alleen worden gemaakt met inachtneming van alle omstandigheden van het afzonderlijke geval. De beoordeling kan daarom per geval anders uitpakken. Technologische ontwikkelingen staan niet stil. Deze beleidsregels zijn derhalve geen statisch document: ze zullen door de Autoriteit Persoonsgegevens zoveel mogelijk actueel gehouden worden.

1. Algemene uitgangspunten verwerking persoonsgegevens door middel van camera's

Op de verwerking van persoonsgegevens door middel van een camera kunnen diverse wettelijke regelingen van toepassing zijn, zoals onder meer de Wet bescherming persoonsgegevens (Wbp), artikel 151c Gemeentewet en de Wet politiegegevens (Wpg). Welke wettelijke regelingen in een concreet geval gelden, is afhankelijk van de vragen wie als verantwoordelijke kan worden aangemerkt en voor welke doeleinden een camera wordt ingezet. Vanuit deze wettelijke regelingen is een aantal uitgangspunten te noemen dat algemeen geldt wanneer persoonsgegevens worden verwerkt door middel van een camera.

[2] Het College bescherming persoonsgegevens wordt sinds 1 januari 2016 in het maatschappelijk verkeer aangeduid als de Autoriteit Persoonsgegevens.

[3] Wijziging van de Gemeentewet in verband met de verruiming van de bevoegdheid van de burgemeester tot de inzet van cameratoezicht, Kamerstukken 33 582.

1.1 Algemene uitgangspunten cameratoezicht

Onderstaande uitgangspunten moeten in elk geval in acht worden genomen voordat een camera wordt ingezet.

1. Stel vast wie de verantwoordelijke zal zijn voor het verwerken van persoonsgegevens door middel van een camera. De verantwoordelijke is degene die deze uitgangspunten in acht moet nemen. Hij is de zogenoemde normadressaat. In het algemeen geldt dat degene die beslist over de doeleinden en de inzet van een camera als verantwoordelijke wordt aangemerkt.[4] Er kunnen meerdere verantwoordelijken zijn.[5] In sommige gevallen is wettelijk bepaald wie als verantwoordelijke wordt aangemerkt.[6]

> **Voorbeeld verantwoordelijke**
> Een winkelier wil cameratoezicht instellen ter beveiliging van de bezoekers[1] en goederen van zijn winkel. De winkelier is degene die beslist dat cameratoezicht wordt ingesteld en voor welk doeleinde. De winkelier wordt derhalve als verantwoordelijke aangemerkt (artikel 1, sub d, Wbp).

[1] In deze beleidsregels wordt met 'bezoekers' bedoeld iedereen die de ruimte bezoekt waarop het betreffende cameratoezicht plaatsvindt, dus ook bijvoorbeeld de verantwoordelijke zelf en werknemers.

> **Voorbeeld verantwoordelijke**
> Een gemeente wil cameratoezicht instellen ter handhaving van de openbare orde. De burgemeester is degene die beslist dat cameratoezicht wordt ingesteld en voor welk doeleinde (artikel 151c Gemeentewet). De burgemeester wordt derhalve als verantwoordelijke aangemerkt.

> **Voorbeeld verantwoordelijke**
> Een gemeente wil verborgen cameraobservatie instellen om de juistheid van de gegevens die noodzakelijk zijn voor de verlening of voortzetting van bijstand te onderzoeken (een zogenoemd bestuurlijk rechtmatigheidsonderzoek).[1] Het college van burgemeesters en wethouders (college van B en W) is degene die beslist dat cameraobservatie wordt ingesteld en voor welk doeleinde (Artikel 53a, lid 6, Wet werk en bijstand). Het college van B en W wordt daarom als verantwoordelijke aangemerkt.

[1] De inzet van verborgen cameraobservatie voor een bestuurlijk rechtmatigheidsonderzoek is slechts in bepaalde, uitzonderlijke gevallen, rechtmatig. Gemeenten die verborgen camera's willen inzetten om uitkeringsfraude op te sporen, moeten de procedure voor de verwerking van de persoonsgegevens (de camerabeelden) vooraf laten onderzoeken door de Autoriteit Persoonsgegevens. Het toenmalige CBP heeft op 30 september 2013 het betreffende protocol van de gemeente Nijmegen goedgekeurd (z2012-00471, autoriteitpersoonsgegevens.nl). Dit protocol kan als voorbeeld dienen voor andere gemeenten die ook verborgen cameraobservatie willen inzetten. Gemeenten die aangeven het Nijmeegse protocol onverkort te volgen, kunnen een aanzienlijk kortere onderzoeksprocedure bij de Autoriteit Persoonsgegevens doorlopen.

> **Voorbeeld verantwoordelijke**
> De politie wil in het kader van de uitoefening van zijn politietaak cameratoezicht instellen. De Wpg bepaalt dat de verantwoordelijke bij de politie de korpschef is (artikel 1, sub f, onder 1, Wpg).

2. Bepaal de doeleinden van de inzet van een camera. Benoem expliciet zowel de hoofddoelen als de nevendoelen, zodat er geen twijfel over bestaat waarvoor een camera zal worden ingezet. Voor overheden is het doel gerelateerd aan de wettelijke taak van de betreffende overheidsorganisatie.

> **Voorbeeld doeleinde**
> Een gerechtvaardigd doeleinde voor cameratoezicht kan zijn de beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen die aan de zorg van de verantwoordelijke zijn toevertrouwd. Dit geldt zowel voor bedrijven en particulieren als voor overheidsorganisaties.

> **Voorbeeld doeleinde**
> De burgemeester is belast met de handhaving van de openbare orde (artikel 172 Gemeentewet). De burgemeester kan ter handhaving van de openbare orde cameratoezicht instellen (artikel 151c Gemeentewet). Het doel van het cameratoezicht is in dit geval dus gerelateerd aan de wettelijke taak van de burgemeester.

> **Voorbeeld doeleinde**
> De politie heeft tot taak te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven (artikel 3 Politiewet 2012).[1] De politie kan ter handhaving van de rechtsorde cameratoezicht instellen. Het doel van het cameratoezicht is in dit geval dus gerelateerd aan de wettelijke taak van de politie.

[1] Het gaat in dit geval om kortstondig cameratoezicht.

3. Stel vast op welke grondslag een camera zal worden ingezet. De verwerking van persoonsgege-

---

[4] Zie over het begrip 'verantwoordelijke' als bedoeld in de Wbp, paragraaf 2.3 'Verantwoordelijke'.

[5] Bijvoorbeeld ingeval van gezamenlijk cameratoezicht door een private organisatie en een gemeente. Zie hierover paragraaf 4.2 'Video-opnames van private goederen en openbare plaatsen door private organisaties en gemeenten'.

[6] Bijvoorbeeld in het geval van cameratoezicht ter handhaving van de openbare orde. Zie hierover paragraaf 3.3 'Verantwoordelijke'.

vens door middel van een camera mag alleen plaatsvinden indien daarvoor een grondslag in de zin van de Wbp aanwezig is. Artikel 8 Wbp noemt zes algemene grondslagen.[7] In sommige gevallen geldt een specifieke wettelijke grondslag.[8]

> **Voorbeeld grondslag**
> Een organisatie wil cameratoezicht instellen ter beveiliging van zijn bezoekers en goederen. De grondslag voor dit cameratoezicht kan zijn artikel 8, sub f, Wbp: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de organisatie.

> **Voorbeeld grondslag**
> Een gemeente wil cameratoezicht instellen ter handhaving van de openbare orde. Voor dit cameratoezicht geldt een specifieke wettelijke grondslag (artikel 8, sub c, Wbp), namelijk artikel 151c Gemeentewet en de betreffende verordening van de gemeenteraad.

4. Stel vast dat de inzet van een cameratoezicht noodzakelijk is. De inzet van een camera moet noodzakelijk zijn om de gestelde doeleinden te kunnen bereiken. Hierbij moeten de belangen van de betrokkenen worden meegewogen. Op deze belangen mag namelijk geen onevenredige inbreuk worden gemaakt in verhouding tot de gestelde doeleinden (proportionaliteit). Als de doeleinden bovendien op een andere wijze kunnen worden verwezenlijkt die minder nadelig is voor de betrokkenen, dan is het betreffende cameratoezicht niet toegestaan (subsidiariteit).[9]

> **Voorbeeld niet noodzakelijk**
> Een restauranthouder wil cameratoezicht instellen, omdat er geregeld geld uit de kassa wordt vermist. Het is voor dit doel *niet* noodzakelijk dat het gehele restaurant wordt gefilmd. Volstaan kan worden met video-opnames van de kassa.

> **Voorbeeld niet noodzakelijk**
> Een gemeente wil cameratoezicht instellen, omdat er geregeld wanordelijkheden zijn in het uitgaansgebied van het centrum. Het is voor dit doel *niet* noodzakelijk dat het gehele centrum wordt gefilmd. Volstaan kan worden met cameratoezicht van het gebied waar de wanordelijkheden plaatsvinden.

5. Bepaal welk soort camera of softwaretechniek in het concrete geval gerechtvaardigd is om in te zetten. De ene camera of softwaretechniek kan een grotere inbreuk op de persoonlijke levenssfeer maken dan de andere. Ook hierbij moeten de belangen van de betrokkenen worden meegewogen (proportionaliteit en subsidiariteit).[10]

> **Voorbeeld inbreuk op de persoonlijke levenssfeer**
> Een camera die is bevestigd aan een drone maakt eerder een grotere inbreuk op de persoonlijke levenssfeer dan een statische camera. Drones kunnen personen namelijk makkelijk volgen en cameratoezicht toepassen op plaatsen waar die personen verwachten onbespied te zijn. Het cameratoezicht door middel van drones is vaak ook niet zichtbaar. Indien dus het doel van het cameratoezicht ook kan worden bereikt op een voor de burger minder ingrijpende wijze, bijvoorbeeld door middel van statische camera's, dan is de inzet van drones (of andere flexibele camera's) niet gerechtvaardigd.

6. Bepaal wat er met de camerabeelden zal worden gedaan. Aan wie zullen de beelden worden verstrekt? Hoe lang zullen de beelden worden bewaard?[11] De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen.
7. Zorg ervoor dat de camerabeelden adequaat zullen worden beveiligd.[12] Maak hierbij gebruik van algemeen geaccepteerde beveiligingsstandaarden. Controleer vervolgens periodiek of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Evalueer tevens periodiek of de getroffen beveiligingsmaatregelen nog voldoende zijn. Pas waar nodig de beveiligingsmaatregelen aan.[13]
8. Bepaal of, en zo ja, op welke wijze, de betrokkenen moeten worden geïnformeerd over de inzet van cameratoezicht.[14] Het adequaat informeren van de betrokkenen over de inzet van cameratoezicht is een belangrijk instrument om de gegevensverwerking transparant te maken. De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen, bijvoorbeeld over het moment van informeren en de inhoud van de informatie.

> **Voorbeeld informeren betrokkenen**
> Een winkelier wil cameratoezicht instellen ter beveiliging van de bezoekers en goederen van zijn winkel. De winkelier zal de betrokkenen over het cameratoezicht informeren door middel van een bord bij de ingang van de winkel.

---

[7] Zie over de grondslagen zoals genoemd in artikel 8 Wbp, paragraaf 2.6 'Grondslagen'.
[8] Bijvoorbeeld in het geval van cameratoezicht ter handhaving van de openbare orde. Zie hierover paragraaf 3.6 'Grondslag'.
[9] Zie over het onderwerp noodzaak, proportionaliteit en subsidiariteit paragraaf 2.7 en 3.7 'Noodzakelijkheid, proportionaliteit en subsidiariteit'.
[10] Camera's kunnen bijvoorbeeld aan drones (onbemande luchtvaartuigen) worden gekoppeld of 'slim' of 'intelligent' zijn, waardoor de camera's niet slechts 'waarnemen', maar ook informatie genereren. Zie hierover hoofdstuk 5 'Drones, dashcams en slimme camera's'.
[11] Zie over het onderwerp bewaartermijnen paragraaf 2.9 en 3.9 'Bewaartermijn'.
[12] Zie over het onderwerp beveiliging paragraaf 2.10 en 3.10 'Beveiliging'.
[13] Dit is de zogenoemde 'plan-do-check-act cyclus'. Zie voor meer informatie over beveiliging de CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013.
[14] Zie over het onderwerp informeren betrokkenen paragraaf 2.13 en 3.13 'Informeren betrokkenen'.

Voorbeeld informeren betrokkenen
Een gemeente wil cameratoezicht instellen ter handhaving van de openbare orde. De gemeente zal de betrokkenen over het cameratoezicht informeren door middel van borden aan de randen van het cameragebied.

Voorbeeld van niet-informeren betrokkenen
Bij een bezoek aan de balie van een kantoor van de Belastingdienst heeft een cliënt de medewerker gefilmd met zijn mobiele telefoon. Deze filmopnamen zijn op YouTube geplaatst. De medewerker is herkenbaar in beeld gebracht, evenals zijn naam en stem. De medewerker is niet geïnformeerd door de cliënt en dat had wel gemoeten.

9. Houd er rekening mee dat de betrokkenen hun rechten, zoals het recht op inzage of correctie, kunnen uitoefenen. De betrokkenen hebben diverse rechten jegens de verantwoordelijke die camerabeelden van hen maakt.[15] Zo hebben de betrokkenen bijvoorbeeld recht op inzage van hun persoonsgegevens en kunnen zij de verantwoordelijke in bepaalde gevallen verzoeken om hun gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen.

1.2 Aandachtspunten

Hieronder volgen nog een tweetal punten waar een verantwoordelijke aan zou moeten denken bij de inzet van cameratoezicht.

Privacy impact assessment (PIA)

Het (laten) uitvoeren van een PIA kan de verantwoordelijke helpen om te voldoen aan voornoemde uitgangspunten en de toepasselijke wettelijke normen. Een PIA is een hulpmiddel voor een verantwoordelijke om door middel van een vragenlijst de privacyrisico's van een (voorgenomen) verwerking in kaart te brengen. Verschillende brancheorganisaties hebben handreikingen voor het uitvoeren van een PIA opgesteld.

Aan de hand van een PIA kan de verantwoordelijke de risico's beoordelen die de verwerking van persoonsgegevens door middel van een camera met zich meebrengt voor de rechten en vrijheden van de betrokkenen. Ook kan hij aan de hand van een PIA maatregelen treffen om deze risico's te beperken. Hierdoor kan de verantwoordelijke de negatieve gevolgen die deze verwerking met zich mee kunnen brengen voor de betrokkenen, maar ook voor hemzelf, zo veel mogelijk beperken. Een PIA is het meest doeltreffend als deze wordt uitgevoerd *voordat* een camera wordt ingezet. Ook als de omstandigheden met betrekking tot de inzet van een camera wijzigen (bijvoorbeeld een wijziging van de doeleinden of de omvang van het toezicht of hetgeen er met de camerabeelden zal worden gedaan), is het raadzaam om opnieuw een PIA uit te voeren.[16]

Uitzondering persoonlijk en huishoudelijk gebruik

De Wbp, waarin de eerder genoemde uitgangspunten zijn opgenomen, is niet van toepassing op de verwerking van persoonsgegevens door middel van een camera ten behoeve van activiteiten met *uitsluitend* persoonlijke of huishoudelijke doeleinden (artikel 2, lid 2, sub a, Wbp). Het *huiselijk gebruik* ziet op de situatie dat in een gezinssituatie persoonsgegevens worden verwerkt. Ook wanneer meerdere personen die gezamenlijk een huishouden voeren, gebruik maken van deze gegevens, is de Wbp niet van toepassing. Om een beroep te doen op deze uitzondering moet het wel gaan om een duidelijk bepaalbare groep van personen.[17] Het *persoonlijk gebruik* ziet zowel op de situatie buiten het werk als daarbinnen. Veel beroepsbeoefenaars houden eigen lijstjes bij, bijvoorbeeld adressenbestanden van personen met wie zij regelmatig contact onderhouden. Zij hebben het karakter van een geheugensteun en deze vallen daarmee onder de uitzondering van het persoonlijk gebruik. Ook camerabeelden gemaakt ter beveiliging in een woning vallen onder deze uitzondering.[18] Zodra deze verwerking beoogd is voor gebruik door een onbepaald aantal personen, is de Wbp van toepassing.[19] Hiervan is bijvoorbeeld sprake indien de camerabeelden op het internet worden geplaatst.[20] Voor betrokkenen is het van belang dat indien de Wbp van toepassing is (en dus geen sprake is van een gebruik voor uitsluitend persoonlijke of huishoudelijke doeleinden) dat zij hun rechten (in de zin van de Wbp) kunnen uitoefenen. Te denken valt aan het recht op inzage, om te corrigeren of te verwijderen. Bij het ongewenst plaatsen van camerabeelden op internet, waarbij de betrokkene in beeld komt,

[15] Zie over het onderwerp rechten van de betrokkenen paragraaf 6.1 'Rechten van betrokkenen'.
[16] Zie voor meer informatie over het uitvoeren van een PIA de website van de Autoriteit Persoonsgegevens: autoriteitpersoonsgegevens.nl.
[17] *Kamerstukken II* 1997/98, 25 892. nr. 3, p. 70.
[18] HvJ EU 11 december 2014, C-212/13 (*Ryneš/ Úřad pro ochranu osobních údajů*).
[19] *Kamerstukken II* 1997/98, 25 892. nr. 3, p. 70.
[20] HvJ EG 6 november 2003, C-101/01 (*Lindqvist*), overweging 47.

kan de betrokkene bij diegene die deze beelden op internet heeft geplaatst (de verantwoordelijke) verzoeken om verwijdering.

In december 2014 heeft het Hof van Justitie een uitspraak gedaan over de uitzondering persoonlijk en huishoudelijk gebruik. Deze uitspraak stelt voorwaarden aan – of de uitzondering wel/niet van toepassing is – het *doorlopend vastleggen* van *(gedeelten) van openbare ruimte* met een *vaste/statische camera* voor het doeleinde: *beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen.*[21] Voor het deel openbare ruimte dat gefilmd wordt voor beveiligingsdoeleinden, heeft het Hof van Justitie bepaald dat geen sprake is van activiteiten met *uitsluitend* persoonlijke of huishoudelijke doeleinden, en daarmee is de Wbp dus onverkort van toepassing.[22] De camera is immers geplaatst met als doel de beveiliging van de woning en dat kan in beginsel niet samenvallen met het doeleinde persoonlijk en huishoudelijk gebruik. De bewoner (verantwoordelijke) dient een grondslag in de zin van artikel 8 Wbp voor zijn verwerking te hebben. Dit zou het gerechtvaardigde belang (artikel 8 aanhef en onder f Wbp) kunnen zijn: de bewoner *kan* een gerechtvaardigd belang hebben om een deel van de openbare ruimte te filmen ter beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen.

Voorbeeld uitsluitend persoonlijk of huishoudelijk gebruik
Een woningeigenaar wil een camera ophangen in zijn woning ter beveiliging van zijn gezin en eigendommen. De camera zal alleen het interieur van de woning filmen. Er is in dit geval sprake van uitsluitend persoonlijk of huishoudelijk gebruik. De bepalingen uit de Wbp zijn daarom *niet* van toepassing.

Voorbeeld uitsluitend persoonlijk of huishoudelijk gebruik
Een woningeigenaar wil een camera ophangen in zijn tuin ter beveiliging van zijn gezin en eigendommen. De camera zal alleen de tuin en *niet* de openbare weg filmen. Er is in dit geval sprake van uitsluitend persoonlijk of huishoudelijk gebruik. De bepalingen uit de Wbp zijn daarom *niet* van toepassing.

Voorbeeld geen uitsluitend persoonlijk of huishoudelijk gebruik
Een woningeigenaar wil een camera ophangen in zijn woning ter beveiliging van zijn gezin en eigendommen. De woningeigenaar heeft een kapsalon aan huis. De camera zal ook de klanten van de kapsalon filmen. Daarmee raakt het cameratoezicht buiten de privésfeer van de woningeigenaar, waardoor er *geen* sprake van uitsluitend persoonlijk of huishoudelijk gebruik. De woningeigenaar moet daarom voldoen aan de bepalingen van de Wbp.

Voorbeeld geen uitsluitend persoonlijk of huishoudelijk gebruik
Een woningeigenaar wil een camera ophangen in zijn tuin ter beveiliging van zijn gezin en eigendommen. De camera zal de tuin en de openbare weg die grenst aan de tuin filmen. Omdat hier de openbare weg wordt gefilmd en er sprake is van filmen voor beveiligingsdoeleinden is de uitspraak van het Hof van Justitie[1] hier van toepassing. Er is dus *geen* sprake is van uitsluitend persoonlijk of huishoudelijk gebruik. Op het filmen van de openbare ruimte is de Wbp onverkort van toepassing.

[1] HvJ EU 11 december 2014, C-212/13 (*Ryneš/ Úřad pro ochranu osobních údajů*), overweging 33 en 35.

Voorbeeld uitsluitend persoonlijk of huishoudelijk gebruik
Een persoon wil een camera aan zijn jas bevestigen (een zogenoemde ‘bodycam’) en daarmee de omgeving voor zichzelf filmen wanneer hij op straat loopt. Op deze beelden zullen ook andere mensen in beeld worden gebracht. Er is sprake van uitsluitend persoonlijk of huishoudelijk gebruik, omdat deze persoon de camerabeelden niet verder verstrekt aan derden. De bepalingen uit de Wbp zijn daarom *niet* van toepassing.

Voorbeeld geen uitsluitend persoonlijk of huishoudelijk gebruik
Een moeder maakt met haar smartphone een film van haar kinderen in de openbare speeltuin. Op deze camerabeelden worden ook andere kinderen in beeld gebracht. Deze moeder zet deze camerabeelden bij thuiskomst op YouTube. Daarmee raakt het cameratoezicht buiten de privésfeer van deze moeder, waardoor er sprake van uitsluitend persoonlijk of huishoudelijk gebruik is. De Wbp is van toepassing.

Uiteraard zijn er gevallen waarbij een persoon de intentie had om een beeldopname te maken voor huishoudelijk gebruik, maar dat deze intentie door bepaalde omstandigheden verandert. Op het moment dat de intentie verandert kan vervolgens de Wbp van toepassing zijn. Deze is dan van toepassing op de verdere verwerking van de beeldopnames.

[21] HvJ EU 11 december 2014, C-212/13 (*Ryneš/ Úřad pro ochranu osobních údajů*), overweging 36.
[22] HvJ EU, 11 december 2014, C-212/13 (*Ryneš/ Úřad pro ochranu osobních údajů*), overweging 33 en 35.

Voorbeeld geen uitsluitend persoonlijk of huishoudelijk gebruik
Een moeder maakt met haar smartphone een film van haar kinderen in de openbare speeltuin. Op deze camerabeelden worden ook andere kinderen in beeld gebracht. Ongewild filmt deze moeder een inbraak van een woning achter de speeltuin. De intentie van de moeder was op voorhand niet om deze beelden verder te verstrekken aan derden, maar doordat ze onbedoeld de woninginbraak filmt en deze beelden aan de politie verstrekt is er sprake van verdere verstrekking aan derden. Daardoor raakt het cameratoezicht buiten de privésfeer van deze moeder, waardoor er vanaf dat moment *geen* sprake meer is van uitsluitend persoonlijk of huishoudelijk gebruik. De Wbp is van toepassing.

Uitwerking uitgangspunten in hoofdstuk 2 en 3

In hoofdstuk 2 worden bovengenoemde uitgangspunten (en andere wettelijke bepalingen) uitgewerkt met betrekking tot cameratoezicht ter beveiliging van personen en goederen (Wbp). In hoofdstuk 3 gebeurt dat met betrekking tot cameratoezicht ter handhaving van de openbare orde door gemeenten (artikel 151c Gemeentewet j° Wpg).

2. Uitwerking Wbp

Dit hoofdstuk bevat een uitwerking van bepalingen van de Wbp die een belangrijke rol spelen bij de verwerking van persoonsgegevens door middel van cameratoezicht. Paragraaf 2.1 tot en met 2.4 hebben betrekking op een aantal algemene begrippen. Paragraaf 2.5 tot en met 2.13 lichten een aantal inhoudelijke normen toe die de verantwoordelijke moet naleven.

2.1 Persoonsgegevens[23]

De Wbp kan alleen van toepassing zijn als er sprake is van ofwel een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens ofwel een niet geautomatiseerde verwerking van persoonsgegevens in een bestand. In deze paragraaf wordt nader uitgewerkt wat onder het begrip ‘persoonsgegevens’ wordt verstaan.

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1, sub a, Wbp).

‘Geïdentificeerde of identificeerbare’

Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.[24] Er kan een onderscheid worden gemaakt in direct en indirect identificeerbare gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificeerbare gegevens is sprake wanneer zij via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.[25]

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.[26]

Ingeval van cameratoezicht zal meestal sprake zijn van persoonsgegevens, aangezien personen vaak herkenbaar in beeld worden gebracht. Maar ook als personen niet of niet herkenbaar in beeld worden gebracht, kan er sprake zijn van persoonsgegevens, zolang de beelden betrekking hebben op een natuurlijke persoon en die persoon *identificeerbaar* is. In onze huidige samenleving met de alle technologische mogelijkheden zal er over het algemeen snel sprake zijn van identificeerbaarheid.

Voorbeeld persoonsgegevens
In een stationshal worden video-opnames gemaakt ter beveiliging van de bezoekers en goederen. Er is in dit geval sprake van persoonsgegevens, aangezien de bezoekers van de stationshal herkenbaar in beeld worden gebracht.

Voorbeeld persoonsgegevens
Een organisatie voor het behoud van de Nederlandse natuur wil video-opnames maken van het Nederlandse natuurlandschap. Daarbij worden onbedoeld ook wandelaars gefilmd. Er is in dit geval sprake van persoonsgegevens, aangezien de wandelaars herkenbaar in beeld worden gebracht. De bedoeling van de organisatie doet hieraan niets af.

[23] Zie voor meer informatie over dit onderwerp WP29, Advies 4/2007 over het begrip persoonsgegeven, WP136, 20 juni 2007.
[24] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.
[25] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48.
[26] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.

Voorbeeld persoonsgegevens
Een school toont camerabeelden van de lessen op haar website. De gezichten van de leerlingen en leerkrachten zijn onherkenbaar in beeld gebracht. De leerlingen herkennen echter één van hun leerkrachten aan zijn opvallende kleding. Er is in dit geval voor deze leerlingen sprake van persoonsgegevens, aangezien de leerlingen (indirect) hun leerkracht kunnen identificeren.

Voorbeeld persoonsgegevens
Een deurwaarder scant door middel van een camera kentekens van auto's. De gescande kentekens worden real time vergeleken met een bestand waarin de gegevens staan van debiteuren tegen wie een vonnis is gewezen. Een 'hit' geeft de deurwaarder de mogelijkheid om het vonnis te executeren. De deurwaarder heeft vanuit zijn beroepstaak toegang tot het kentekenregister van de Rijksdienst voor het Wegverkeer (RDW). Hierdoor kan de deurwaarder (indirect) een persoon identificeren. De kentekens zijn daarom in ieder geval voor de deurwaarder persoonsgegevens.

2.2 Verwerking

De Wbp is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2 lid 1 Wbp). In deze paragraaf wordt nader uitgewerkt wat onder het begrip '*verwerking*' wordt verstaan.

Een verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

Bij digitale camera's worden intern geheugen en een digitale processor gebruikt om de beeldgegevens op te slaan en door te zetten tussen verschillende componenten van het systeem. Dus wordt dat dit proces – hoe tijdelijk ook van karakter – altijd wordt beschouwd als een verwerking in de zin van de Wbp. Het actief gebruik van opnamefunctionaliteiten is niet relevant om te bepalen of er sprake zal zijn van een verwerking in de zin van de Wbp. Dit betekent dat er bij het gebruik van een digitale camera altijd een verwerking van persoonsgegevens plaatsvindt, ook als beelden niet actief worden vastgelegd. Daarmee is het live uitkijken middels een digitale camera een verwerking van persoonsgegevens en is de Wbp van toepassing.[27][28]

Voorbeeld geen verwerking
Een winkelier heeft als afschrikmiddel tegen diefstal dummy-camera's in zijn winkel hangen. Een dummy-camera is geen echte camera en neemt geen beelden op. De Wbp is op deze situatie niet van toepassing

Voorbeeld verwerking
Een winkelier heeft cameratoezicht ingesteld ter beveiliging van zijn goederen. De camerabeelden worden niet vastgelegd, maar wel live uitgekeken door daartoe bevoegd winkelpersoneel. De Wbp is ook op deze situatie van toepassing.

Voorbeeld verwerking
Een onderneming maakt video-opnames van een recreatiepark. De bezoekers van het park worden hierbij herkenbaar in beeld gebracht. Nadat de beelden van de bezoekers dusdanig zijn geblurd[1] zodat de bezoekers niet meer identificeerbaar zijn, worden de opnames op de website van de onderneming geplaatst. De onderneming verwerkt persoonsgegevens met het opnemen en blurren van de beelden.

1 Blurren is het wazig maken van afbeeldingen.

Voorbeeld verwerking
Een kerk toont camerabeelden van een uitvaartplechtigheid via een livestreamverbinding op internet. Daarbij komen ook identificeerbare personen in beeld. De camerabeelden worden niet opgenomen. Ondanks dat er niet actief video-opnames worden gemaakt, is de Wbp toch van toepassing.

---

27 Mits uiteraard aan de overige eisen voor de verwerking van persoonsgegevens is voldaan, zoals dat het beelden van identificeerbare of geïdentificeerde personen betreft.
28 Voorheen was door het gebruik van analoge camera's geen sprake van een verwerking van persoonsgegevens, doordat de analoge camera's niet voorzien waren van digitale processoren. Tegenwoordig zijn bij de digitale camera's die in de omloop zijn deze standaard voorzien van digitale processoren, waardoor reeds daarom sprake is van verwerking van persoonsgegevens.

Voorbeeld verwerking
Een verkeerscentrale heeft cameratoezicht ingesteld om toezicht te houden op de actuele verkeersafwikkeling. Als er een incident plaatsvindt, stuurt de verkeerscentrale de camerabeelden, waarop persoonsgegevens zichtbaar zijn, live door naar de politie. Hierdoor kan de politie rechtstreeks meekijken wat er aan de hand is. Zowel het vastleggen van beelden als het doorsturen van de camerabeelden aan de politie is een verwerking van persoonsgegevens.

Voorbeeld verwerking
Middels een smartphone-applicatie streamt een bezoeker live beelden van een evenement. De bezoekers van het evenement worden hierbij herkenbaar in beeld gebracht. Alle andere gebruikers van deze applicatie kunnen de beelden bekijken. Ondanks dat er geen camerabeelden worden vastgelegd op de smartphone, is de Wbp toch van toepassing.

2.3 Verantwoordelijke[29]

De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp).

De vraag die hierbij mede van belang is, is wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval er sprake van gezamenlijke verantwoordelijkheid.[30]

Ten aanzien van cameratoezicht geldt veelal dat degene die beslist over de inzet van cameratoezicht kan worden aangemerkt als de verantwoordelijke in de zin van de Wbp.

2.4 Bewerker[31]

De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1, sub e, Wbp).

De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon of instelling. Het zal veelal gaan om een persoon of instelling die niet in een hiërarchische relatie tot de verantwoordelijke staat. Daar waar een hiërarchische relatie bestaat met de verantwoordelijke moet worden gesproken van (intern) beheer. Tevens geldt dat de bewerker gegevens verwerkt ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. Voorts beperkt de bewerker zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt dus geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag van de gegevens etcetera.[32]

De verantwoordelijke die persoonsgegevens wil laten verwerken door een bewerker moet een overeenkomst met de bewerker sluiten waarin de uitvoering van de verwerkingen wordt geregeld (artikel 14, lid 2, Wbp).

Voorbeeld bewerker
Een directeur van bedrijf X heeft camera's opgehangen ter beveiliging van zijn bedrijf, eigendommen en personeel. De directeur van bedrijf X laat de beelden uitkijken door (een extern) bedrijf Y. Bedrijf Y kijkt de beelden uit in opdracht van bedrijf X. Hiertoe heeft bedrijf X bedrijf Y een bewerkersovereenkomst laten ondertekenen, waarin expliciet vermeld staat wat bedrijf Y met de camerabeelden mag doen.

2.5 Doeleinden[33]

Persoonsgegevens mogen slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7 Wbp). Dit betekent dat de verantwoordelijke één of meer duidelijk omlijnde doelen moet vaststellen voordat hij met de verwerking aanvangt. De doelomschrijving mag niet zo vaag of ruim zijn dat zij tijdens het verwerkingsproces geen kader kan bieden waaraan getoetst kan worden of de betreffende persoonsgegevens nodig zijn voor de omschreven

[29] Zie voor meer informatie over dit onderwerp WP29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', WP169, 16 februari 2010.
[30] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 55.
[31] Zie voor meer informatie over dit onderwerp WP29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', WP169, 16 februari 2010.
[32] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 61.
[33] Zie voor meer informatie over dit onderwerp WP29, Opinion 03/2013 on purpose limitation, WP203, 2 april 2013.

doeleinden of niet.[34] De doeleinden mogen ook niet in de loop van het verwerkingsproces worden geformuleerd. Bovendien moeten de doeleinden gerechtvaardigd zijn. Dit houdt in dat het belang van de verantwoordelijke redelijkerwijs aanleiding dient te geven om de betreffende persoonsgegevens voor de omschreven doeleinden te mogen verwerken. Tevens mag de verwerking van de persoonsgegevens niet in strijd zijn met enige wet, de openbare orde of de goede zeden.[35]

Voorbeeld doeleinde gerechtvaardigd
Een supermarkt heeft cameratoezicht ingezet 'ter beveiliging van zijn eigendommen tegen diefstal'. De beveiliging van eigendommen kan een gerechtvaardigd doeleinde zijn om cameratoezicht in te stellen.

Voorbeeld doeleinde niet welbepaald
Een winkelier heeft cameratoezicht ingezet ter 'observatie van zijn klanten'. Het doeleinde 'observatie van klanten' is te vaag en ruim geformuleerd en daarmee niet welbepaald. De winkelier moet omschrijven voor welke doeleinden de klanten worden geobserveerd.

2.6 Grondslagen

Artikel 8 Wbp noemt zes grondslagen voor het mogen verwerken van persoonsgegevens. Deze zijn, kort weergegeven:
a. ondubbelzinnige toestemming van de betrokkene[36];
b. uitvoering van een overeenkomst;
c. wettelijke verplichting;
d. vrijwaring van een vitaal belang van de betrokkene;
e. publiekrechtelijke taak;
f. gerechtvaardigd belang, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene prevaleert[37].

De gegevensverwerking moet op (minimaal) één van deze grondslagen berusten. Artikel 8 Wbp behelst bovendien dat bij elke verwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit.[38] Hieronder, in paragraaf 2.7, wordt nader ingegaan op deze beginselen.

Vrijwaring van een vitaal belang

De grondslag 'vrijwaring van een vitaal belang' (sub d) zal voor cameratoezicht ter beveiliging van personen en goederen meestal *niet* gelden. Deze grondslag moet namelijk eng worden geïnterpreteerd: er moet een dringende medische noodzaak aanwezig zijn om de gegevens van de betrokkene te verwerken. Het moet gaan om een zaak van leven of dood.[39]

Publiekrechtelijke taak

Aan bestuursorganen zijn bij of krachtens de wet publiekrechtelijke taken toegekend. Voor een goede vervulling van een publiekrechtelijke taak kan het noodzakelijk zijn dat het betreffende bestuursorgaan cameratoezicht instelt (sub e).

Gerechtvaardigd belang

Voor cameratoezicht ter beveiliging van personen en goederen zou de grondslag 'gerechtvaardigd belang' (sub f) kunnen gelden. Het belang van de verantwoordelijke om cameratoezicht in te stellen moet dan zwaarder wegen dan de belangen van de betrokkenen. Tevens moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit.

[34] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 79.
[35] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 78.
[36] Zie voor meer informatie over dit onderwerp WP29, Advies 15/2011 over de definitie van 'toestemming', WP187, 13 juli 2011.
[37] Zie voor meer informatie over dit onderwerp WP29,
Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, WP217, 9 april 2014.
[38] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80.
[39] Als voorbeeld kan de situatie gelden dat terstond medische hulp nodig is naar aanleiding van een ongeval van de betrokkene waarbij deze buiten bewustzijn is geraakt. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 84.

Voorbeeld geen gerechtvaardigd belang
Een onderneming heeft Mystery Shopping met verborgen camera's ingezet. De camera's filmen het personeel in het kader van een training. De onderneming beroept zich op de grondslag 'gerechtvaardigd belang' (artikel 8, sub f, Wbp). Voor een geslaagd beroep op een gerechtvaardigd belang, moeten de belangen van de onderneming zwaarder wegen dan de belangen van het personeel. De inbreuk op de privacy van werknemers is bij deze methode echter dermate groot, dat het belang van de onderneming om het personeel te trainen middels heimelijk cameraobservatie ondergeschikt is aan het belang van het personeel om zijn werk uit te voeren zonder onderworpen te zijn aan heimelijke cameraobservaties. Het beroep op de grondslag 'gerechtvaardigd belang' slaagt in dit geval dus niet.

2.7 Noodzakelijkheid, proportionaliteit en subsidiairiteit

Een belangrijk vereiste van een rechtmatige verwerking van persoonsgegevens door middel van cameratoezicht betreft de noodzakelijkheid van de verwerking. Hierbij spelen de beginselen van proportionaliteit en subsidiariteit een belangrijke rol.
Het proportionaliteitsbeginsel houdt in dat de inbreuken op de belangen van de betrokkenen niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel.[40] Ingevolge het subsidiariteitsbeginsel moet het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de betrokkenen minder nadelige, wijze kunnen worden verwerkelijkt.[41]

Concreet betekent het vorenstaande dat cameratoezicht ter beveiliging van personen en goederen slechts mag worden ingezet indien er ook andere beveiligingsmaatregelen zijn getroffen. Minder vergaande maatregelen dienen onvoldoende effectief te zijn en deze maatregelen kunnen redelijkerwijs niet worden uitgebreid. Tevens mogen er niet meer en langer camera's worden ingezet en niet meer personen en/of plaatsen in beeld worden gebracht dan strikt noodzakelijk is voor de gestelde doeleinden (dataminimalisatie). Dit betekent dat de verantwoordelijke alleen continu cameratoezicht mag instellen wanneer niet kan worden volstaan met opnames gedurende bepaalde periodes.

Cameratoezicht in bijvoorbeeld een toilet, pashokje, kleedkamer of behandelruimte maakt een te grote inbreuk op de persoonlijke levenssfeer van de betrokkenen. In deze ruimten mag een betrokkene redelijkerwijs verwachten onbespied te zijn. Cameratoezicht in deze ruimtes voldoet daarmee niet aan het vereiste van proportionaliteit en is dus niet toegestaan.

Voorts geldt dat het plaatsen van camerabeelden op internet vaak niet noodzakelijk is. De belangen van de betrokkenen kunnen hierdoor immers onevenredig worden geschaad, doordat de beelden voor een ieder toegankelijk zijn (disproportioneel).

De noodzaak van de gegevensverwerking moet aanwezig zijn gedurende het gehele verwerkingsproces en dus niet slechts op het moment dat de verwerking aanvangt. Dit betekent dat de verantwoordelijke zich er regelmatig van moet vergewissen of het cameratoezicht nog steeds noodzakelijk is. Wat 'regelmatig' is, is afhankelijk van de omstandigheden van het concrete geval. Factoren die hierbij een rol kunnen spelen zijn onder andere het doel en de ernst van de situatie waarvoor het cameratoezicht wordt ingesteld, de branche en omgeving waarbinnen de verantwoordelijke zich bevindt en eventuele veranderingen van de omstandigheden.

Heimelijk cameratoezicht

Heimelijk cameratoezicht is in de regel niet toegestaan, aangezien het een grote inbreuk maakt op de persoonlijke levenssfeer. Slechts in bijzondere omstandigheden zal voldaan zijn aan de beginselen van proportionaliteit en subsidiariteit. Hiervan kan sprake zijn ingeval van (een redelijk vermoeden van) diefstal of fraude en andere genomen maatregelen hieraan geen einde hebben kunnen maken. Daarbij geldt dat verborgen cameratoezicht slechts tijdelijk mag worden ingezet.[42]

Is er geen sprake van bijzondere omstandigheden dan is er sprake van een strafbaar feit en kan diegene die gefilmd is door een verborgen camera aangifte bij de politie doen van dit feit ingevolge de artikelen 139f, lid 1, en 441b Wetboek van Strafrecht.

[40] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 8.
[41] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 8–9.
[42] Zie over het informeren van betrokkenen ingeval van heimelijk cameratoezicht paragraaf 2.13 'Informeren betrokkenen'. Cameratoezicht dat niet op een duidelijke wijze kenbaar is gemaakt, is onder omstandigheden strafbaar op grond van artikel 139f, lid 1, en 441b Wetboek van Strafrecht.

Voorbeeld noodzakelijk
Op een parkeerplaats worden 's nachts vaak auto's vernield. De parkeerplaatshouder heeft reeds een hek om de parkeerplaats geplaatst, extra verlichting aangebracht en een beveiligingsbeambte vaker laten surveilleren. Deze maatregelen blijken echter onvoldoende effect te sorteren, waardoor de parkeerplaatshouder heeft besloten tot het inzetten van cameratoezicht. De camera's staan alleen aan gedurende de nachtelijke uren. De parkeerplaatshouder heeft hiermee de noodzaak (proportionaliteit en subsidiariteit) van het cameratoezicht aangetoond.

Voorbeeld niet noodzakelijk
Een onderneming heeft Mystery Shopping met verborgen camera's ingezet. De camera's filmen het personeel in het kader van een training. De onderneming heeft voor de inzet van heimelijke camera's gekozen wegens onvoldoende resultaten van eerdere trainingen. Het leereffect na concrete voorbeelden uit de eigen werksituatie zou volgens de onderneming naar algemene onderwijsinzichten groter zijn dan na alleen een algemeen betoog over verkooptechniek. De onderneming beargumenteert hiermee evenwel niet voldoende waarom het inzetten van heimelijk cameratoezicht het ultimum remedium is om het trainingsdoeleinde te bereiken. Een groter leereffect kan ook anderszins en met minder ingrijpende middelen worden bereikt, bijvoorbeeld door middel van rollenspellen, mystery shoppers zonder heimelijke camera en cursussen klantgerichtheid. Hieruit volgt dat de inzet van heimelijke cameraobservatie niet noodzakelijk is.

2.8 Verdere verwerking[43]

Persoonsgegevens mogen alleen verder worden verwerkt op een wijze die niet onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9, lid 1, Wbp). De vraag of er sprake is van verenigbaarheid wordt *in ieder geval* beoordeeld aan de hand van de volgende factoren (artikel 9, lid 2, Wbp):
1. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
2. de aard van de betreffende gegevens;
3. de gevolgen van de beoogde verwerking voor de betrokkene;
4. de wijze waarop de gegevens zijn verkregen en
5. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

De opsomming is niet limitatief. Bovendien is geen van deze factoren op zichzelf van doorslaggevende betekenis. Elk van de genoemde factoren moet – mogelijk in samenhang met andere factoren die in het concrete geval als relevant moeten worden beschouwd – in onderling verband worden beoordeeld en gewogen ter beantwoording van de vraag of sprake is van verenigbaar gebruik.[44]
De eis van verenigbaar gebruik geldt zowel voor de situatie dat persoonsgegevens verder worden verwerkt binnen de organisatie van de verantwoordelijke als buiten de organisatie van de verantwoordelijke, dus als de gegevens worden verstrekt aan derden. Het doet er bij verdere verwerking binnen de organisatie van de verantwoordelijke eveneens niet toe of deze organisatie bestaat uit één of meerdere ondernemingen dan wel om één of meerdere rechtspersonen.[45]

Voorbeeld onverenigbaar
Een onderneming heeft medewerkers aangesproken op hun functioneren op basis van camerabeelden van beveiligingscamera's. Het gebruik van beelden van beveiligingscamera's voor het controleren van het functioneren van werknemers is onverenigbaar met het oorspronkelijke doel, omdat er geen enkele verwantschap is met het doel van de cameraobservaties, namelijk het waarborgen van de veiligheid van de klant en de medewerker en het zoveel mogelijk voorkomen van winkeldiefstal.

2.9 Bewaartermijn

In het algemeen geldt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verwerkt (artikel 10, lid 1 Wbp).

De Wbp noemt geen specifieke bewaartermijnen. Het Vrijstellingsbesluit Wbp geeft wel een indicatie van een bewaartermijn voor specifieke gegevens. Ten aanzien van duidelijk zichtbaar cameratoezicht ter beveiliging van personen of goederen die zijn toevertrouwd aan de zorg van de verantwoordelijke, noemt het Vrijstellingsbesluit Wbp een bewaartermijn van *maximaal* vier weken dan wel tot een geconstateerd incident is afgehandeld (artikel 38, lid 6, Vrijstellingsbesluit Wbp). Hoewel deze bewaartermijn niet dwingend is, geeft het wel een duidelijke indicatie van de termijn waarbinnen het bewaren van de betreffende persoonsgegevens nog noodzakelijk kan worden geacht. Uiteraard zullen er gevallen zijn waarbij persoonsgegevens minder lang bewaard hoeven te worden dan de maximale termijn van vier weken. Indien de noodzaak tot het bewaren van de persoonsgegevens afwezig is moeten de persoonsgegevens eerder dan de maximale termijn van vier weken verwijderd worden.

[43] Zie voor meer informatie over dit onderwerp WP29, Opinion 03/2013 on purpose limitation, WP203, 2 april 2013.
[44] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 90.
[45] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 89-90.

Voorbeeld incident afgehandeld
Een winkelier heeft cameratoezicht ingesteld ter beveiliging van zijn goederen. Nadat een winkeldiefstal heeft plaatsgevonden, doet de winkelier daarvan aangifte bij de politie en verstrekt hij de politie de betreffende camerabeelden. Het incident (de winkeldiefstal) is in dit geval afgehandeld nadat de strafzaak onherroepelijk is geworden. De winkelier mag de camerabeelden niet langer bewaren.
Hetzelfde geldt ingeval de winkelier een civielrechtelijk geding tegen de winkeldief aanspant om zijn schade vergoed te krijgen. Ook dan is het incident (de winkeldiefstal) in dit geval afgehandeld nadat de civielrechtelijke zaak onherroepelijk is geworden. De winkelier mag de camerabeelden niet langer bewaren.

2.10 Beveiliging[46]

De verantwoordelijke moet de camerabeelden adequaat beveiligen. Artikel 13 Wbp vereist dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act cyclus in de dagelijkse praktijk van de organisatie noodzakelijk.[47]

Een onderdeel van de benodigde beveiliging is het voorkomen dat onbevoegden toegang kunnen krijgen (geautoriseerd zijn) tot de camerabeelden. Hierbij kan onder meer worden gedacht aan het deugdelijk versleutelen van camerabestanden middels encryptie. Welke personen toegang mogen krijgen is afhankelijk van de functie die zij bekleden alsmede de aard van de gegevens en de doeleinden van het cameratoezicht. Hieronder kunnen ook de mensen vallen die onderhoudswerkzaamheden aan de camera-installatie verrichten. De activiteiten die deze personen met de camerabeelden uitvoeren moeten worden gelogd, evenals pogingen van anderen om ongeautoriseerd toegang te krijgen.[48]

Het uitvoeren van een Privacy Impact Assessment (PIA)[49] kan de verantwoordelijke helpen om te bepalen welke beveiligingsmaatregelen noodzakelijk zijn.

Voorbeeld beveiliging
Een bedrijf heeft cameratoezicht ingesteld ter beveiliging van zijn bezoekers en goederen. Onder de personen die toegang mogen krijgen tot de camerabeelden kunnen de beveiligingsfunctionarissen en de medewerkers van de storingsdienst vallen. De administratief medewerkers zullen hier niet onder vallen.

Voorbeeld beveiliging
Een bedrijf heeft cameratoezicht ingesteld ter beveiliging van zijn bezoekers en goederen. Als onderdeel van de beveiliging worden de camerabeelden gedurende de bewaartermijn in een kluis opgeslagen.

Voorbeeld onvoldoende beveiliging
IP-camera's maken gebruik van het Internet-Protocol om camerabeelden te streamen via internet. Indien de toegangsbeveiliging tot deze camerabeelden niet goed is geregeld, is het mogelijk dat een ieder de beelden via internet kan bekijken. Hiervan kan bijvoorbeeld sprake zijn ingeval het standaardwachtwoord van de camera, zoals is ingesteld door de fabriek, niet wordt gewijzigd.

2.11 Bijzondere persoonsgegevens

De Wbp noemt in artikel 16 persoonsgegevens die als bijzonder worden aangemerkt gelet op hun gevoelige karakter. Het betreft de persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging alsmede strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.[50]

---

[46] Zie voor meer informatie over dit onderwerp de CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013 (autoriteitpersoonsgegevens.nl)
[47] CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 14 e.v.
[48] CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22.
[49] Zie over het onderwerp PIA ook Hoofdstuk '1. Algemene uitgangspunten verwerking persoonsgegevens door middel van camera's'.
[50] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 122.

Als hoofdregel geldt dat de verwerking van voornoemde bijzondere persoonsgegevens niet is toegestaan. De artikelen 17 tot en met 23 Wbp bevatten een ontheffing van dit algemene verwerkingsverbod. Eerst worden de bijzondere ontheffingen genoemd (artikel 17 tot en met 22 Wbp) en daarna een algemene slotbepaling (artikel 23 Wbp). Deze artikelen legitimeren niet een gegevensverwerking van bijzondere persoonsgegevens, maar zij doorbreken slechts een verbod. Vervolgens zal dus aan de hand van de overige bepalingen van de Wbp moeten worden vastgesteld of de gegevensverwerking in het concrete geval rechtmatig is.[51]

Op camerabeelden van personen zijn de fysieke kenmerken van die personen zichtbaar. Zo is bijvoorbeeld zichtbaar of iemand een bril draagt (wat iets zegt over zijn visuele gezondheid) of een hoofddoek (wat iets kan zeggen over godsdienstige overtuiging). Tevens kan iemands ras van de camerabeelden worden afgeleid.[52] Dit zou in de praktijk – strikt genomen – betekenen dat álle camerabeelden van personen bijzondere persoonsgegevens zijn. Daarvoor zal in veel gevallen geen uitzondering te vinden zijn in artikel 17 tot en met 23 Wbp, terwijl het betreffende cameratoezicht *an sich* niet als onaanvaardbaar hoeft te worden aangemerkt, hetgeen ook in latere rechtspraak duidelijk wordt.[53] Ook in de Algemene verordening gegevensbescherming wordt dit genuanceerd: '*The processing of photographs will not systematically be a sensitive processing (...).*'[54]

Gelet hierop beschouwt de Autoriteit Persoonsgegevens camerabeelden van een persoon thans, ook om opportuniteitsredenen, *niet* als bijzondere persoonsgegevens als:
- het doeleinde van de verwerking *niet* gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven,
- het voor de verantwoordelijke redelijkerwijs *niet* voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven, en
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking.

Indien de verwerking van camerabeelden echter identificatie tot doel heeft, worden deze beelden wel als een rasgegeven aangemerkt.

Overigens zal het cameratoezicht ter beveiliging van personen of goederen op basis van de bovenstaande criteria meestal *wel* worden aangemerkt als strafrechtelijke gegevens in de zin van artikel 16 en 22 Wbp, aangezien het doeleinde van de verwerking (mede) gericht zal zijn op het verwerken van strafrechtelijke gegevens. Bovendien zal het voor de verantwoordelijke redelijkerwijs voorzienbaar zijn dat het cameratoezicht ertoe zal leiden dat er onderscheid wordt gemaakt ten aanzien van een betrokkene die een strafbaar feit begaat. Het verbod om strafrechtelijke gegevens te verwerken is echter niet van toepassing op de verantwoordelijke die deze gegevens verwerkt ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn[55] (artikel 22, lid 2, sub b, Wbp[56]).

Op basis van de bovenstaande criteria zal cameratoezicht ter beveiliging van personen of goederen meestal *niet* worden aangemerkt als een verwerking van persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging als bedoeld in artikel 16 Wbp.

Voorbeeld *gezondheidsgegevens* die volgens criteria niet worden beschouwd als bijzondere persoonsgegevens
In de hal van een ziekenhuis vindt cameratoezicht plaats ter beveiliging van de bezoekers en goederen van het ziekenhuis. Het feit dat iemand met krukken loopt of in een rolstoel zit is een gegeven over iemands fysieke welzijn en daarmee een gegeven omtrent iemands gezondheid. De camerabeelden worden in dit geval evenwel niet aangemerkt als bijzondere persoonsgegevens *in de zin van artikel 16 en 21 Wbp* (*gezondheidsgegevens*), gelet op de invulling van de bovenstaande criteria:
• Het doel van het cameratoezicht is niet gericht op het vastleggen van gezondheidsgegevens van de bezoekers, maar op beveiliging. Ook wordt middels het cameratoezicht geen onderscheid gemaakt op basis van de gezondheid van de bezoekers.
• Het is voor het ziekenhuis redelijkerwijs niet voorzienbaar dat het cameratoezicht zal leiden tot het maken van onderscheid.
• Het verwerken van de gezondheidsgegevens van de bezoekers van het ziekenhuis is onvermijdelijk bij de inzet van cameratoezicht in een ziekenhuis.

51 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 101.
52 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 105 en HR 23 maart 2010, ECLI:NL:HR:2010:BK6331, r.o. 2.6.
53 Zie onder andere: de Hoge Raad in HR 21 december 2010, ECLI:NL:HR:2010:BL7688.
54 Zie: overweging 41 van de Algemene verordening gegevensbescherming.
55 *Kamerstukken II*, 1997/98, 25 892, p. 120.
56 Artikel 22, lid 2, sub b, Wbp luidt:
Het verbod is niet van toepassing op de verantwoordelijke die deze gegevens ten eigen behoeve verwerkt ter:
(...)
b. *bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.*

Voorbeeld *rasgegevens* die volgens criteria niet worden beschouwd als bijzondere persoonsgegevens
In een winkel vindt cameratoezicht plaats ter beveiliging van de bezoekers en goederen van de winkel. Van de camerabeelden is het ras van de bezoekers af te leiden. De camerabeelden worden in dit geval evenwel niet aangemerkt als bijzondere persoonsgegevens *in de zin van artikel 16 en 18 Wbp* (*rasgegevens*), gelet op de invulling van de bovenstaande criteria:
- Het doel van het cameratoezicht is niet gericht op het vastleggen van de rasgegevens van de bezoekers, maar op beveiliging. Ook wordt middels het cameratoezicht geen onderscheid gemaakt op basis van het ras van de bezoekers.
- Het is voor de winkelier redelijkerwijs niet voorzienbaar dat het cameratoezicht zal leiden tot het maken van onderscheid op basis van een bijzonder persoonsgegeven.
- Het verwerken van de rasgegevens van de bezoekers van de winkel is onvermijdelijk bij de inzet van cameratoezicht in een winkel.
- De verwerking van de camerabeelden heeft geen identificatie tot doel.

2.12 Melden[57]

De Wbp bepaalt in het algemeen dat een voorgenomen verwerking van persoonsgegevens moet worden gemeld bij de Autoriteit Persoonsgegevens of een functionaris voor de gegevensbescherming (artikel 27 Wbp). De melding moet worden gedaan *alvorens* met de verwerking wordt begonnen.

De verwerking van persoonsgegevens door middel van cameratoezicht ten behoeve van beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen hoeft niet te worden gemeld als is voldaan aan de vereisten van artikel 38 Vrijstellingsbesluit Wbp. De belangrijkste vereisten die dit artikel noemt zijn: het cameratoezicht is ingesteld ter beveiliging van personen en goederen die zijn toevertrouwd aan de zorg van de verantwoordelijke, het cameratoezicht is duidelijk zichtbaar en de persoonsgegevens worden verwijderd uiterlijk vier weken nadat de videoopnames zijn gemaakt, dan wel na afhandeling van geconstateerde incidenten.

Het Vrijstellingsbesluit Wbp is niet van toepassing ingeval sprake is van meer dan één verantwoordelijke (artikel 2 Vrijstellingsbesluit Wbp). Dan geldt voornoemde vrijstelling van de meldplicht dus niet en moet de verwerking worden gemeld.

Heimelijk cameratoezicht

Een voorgenomen verwerking van persoonsgegevens door middel van heimelijk cameratoezicht moet *altijd* worden gemeld bij de Autoriteit Persoonsgegevens. Daarbij moet bovendien een voorafgaand onderzoek worden aangevraagd. Het voorafgaand onderzoek houdt in dat de Autoriteit Persoonsgegevens de rechtmatigheid van de voorgenomen verwerking onderzoekt. Met de verwerking mag niet worden begonnen totdat de Autoriteit Persoonsgegevens dit onderzoek heeft afgerond dan wel heeft besloten om geen onderzoek in te stellen.[58]

Voorbeeld melden heimelijk cameratoezicht
Een transportonderneming heeft een redelijk vermoeden dat een werknemer geregeld diefstal pleegt van lading uit een vrachtwagen wanneer hij de lading vervoert. De onderneming wil heimelijk cameratoezicht instellen ten aanzien van de vrachtwagen waarin en de tijdstippen waarop de betreffende werknemer de lading vervoert. De onderneming moet deze voorgenomen verwerking van persoonsgegevens melden bij de Autoriteit Persoonsgegevens en zij moet een voorafgaand onderzoek aanvragen. Het feit dat het heimelijke cameratoezicht slechts op ‘ad hoc basis’ plaatsvindt, doet hieraan niets af.

2.13 Informeren van betrokkenen

In de regel geldt dat betrokkenen moeten worden geïnformeerd dat er cameratoezicht plaatsvindt *alvorens* zij daadwerkelijk worden gefilmd (artikel 34 j° 33 Wbp).

Deze informatieplicht houdt in dat voor de betrokkenen in ieder geval duidelijk moet zijn dat er cameratoezicht plaatsvindt, voor welke doeleinden dit gebeurt en wie daarvoor verantwoordelijk is. Daarnaast moet de verantwoordelijke nadere informatie verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen (artikel 33, lid 3, en 34, lid 3, Wbp).

Het is niet nodig dat precies wordt aangeven waar de camera’s zijn geïnstalleerd, maar wel in welk gebied het cameratoezicht plaatsvindt. Tevens is niet nodig dat de betrokkenen kunnen zien of de camera’s in werking zijn.

---

57 Zie voor meer informatie over het melden van verwerkingen de website van de Autoriteit Persoonsgegevens: autoriteitpersoonsgegevens.nl.
58 Zie voor meer informatie over het voorafgaand onderzoek autoriteitpersoonsgegevens.nl

Indien uit de context duidelijk kan worden afgeleid wat het doel van het cameratoezicht is en wie de verantwoordelijke is, kan een bord met een symbool van een camera voldoende zijn. De verantwoordelijke moet dan desgevraagd wel nadere informatie verstrekken. Het is bovendien aan te bevelen dat informatieverstrekking ook op andere wijzen plaatsvindt, bijvoorbeeld op de website van de verantwoordelijke of door middel van folders.

Deze informatieplicht is niet absoluut. Uitgezonderd is de situatie dat de informatieverstrekking aan de betrokkenen onmogelijk blijkt of een onevenredige inspanning kost. In dat geval moet de verantwoordelijke in ieder geval de herkomst van de gegevens vastleggen (artikel 34, lid 4, Wbp). Dit stelt de betrokkenen in staat achteraf bij de verantwoordelijke na te gaan welke keten van verstrekkingen heeft plaatsgevonden.[59] Zo kunnen camerabeelden afkomstig zijn van de beveiligingscamera's van de verantwoordelijke zelf. Maar het is ook mogelijk dat derden de camerabeelden aan de betreffende verantwoordelijke heeft verstrekt.

Heimelijk cameratoezicht

Eveneens kan de informatieverstrekking buiten toepassing worden gelaten *voor zover* dit *noodzakelijk* is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten (artikel 43, sub b, Wbp). Deze uitzonderingsgrond kan van toepassing zijn op een werkgever die heimelijk cameratoezicht instelt wegens (een redelijk vermoeden van) diefstal of fraude.[60] In die situatie gelden wel de volgende voorwaarden:

- De werkgever moet alle werknemers in algemene termen vooraf informeren over de mogelijke inzet van heimelijk cameratoezicht in de toekomst.[61]
- Indien er een ondernemingsraad (OR) of personeelsvereniging is, dan moet deze ondernemingsraad of personeelsvereniging hebben ingestemd met een regeling ten aanzien van deze verwerking.[62]
- De werkgever moet de werknemers altijd achteraf informeren over het heimelijke cameratoezicht indien hij daartoe daadwerkelijk is overgegaan. De informatieplicht van artikel 34 j° 33 Wbp herleeft namelijk zodra het heimelijk cameratoezicht niet meer noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten. De werkgever moet de betrokkenen (bijvoorbeeld de dader) persoonlijk informeren.

Voorbeeld niet voldaan aan informatieplicht
Direct na de ingang van een winkel hangt een camera. Achter de toonbank van de winkel hangt een bord met de tekst 'Voor uw en onze veiligheid vindt hier camerabewaking plaats'. Deze werkwijze is niet geoorloofd, aangezien de informatieverstrekking moet plaatsvinden voordat de bezoekers van de winkel worden gefilmd. Het bord had daarom zichtbaar moeten zijn vanaf de ingang van de winkel.

Voorbeeld voldaan aan informatieplicht
In een winkel vindt cameratoezicht plaats. Bij de ingang van de winkel, voordat de bezoekers worden gefilmd, hangt een duidelijk bord met een symbool van een camera. Uit de context is duidelijk dat de camera's dienen ter beveiliging van de goederen in de winkel en dat de winkeleigenaar de verantwoordelijke is. Aan de informatieplicht is in dit geval voldaan.

Voorbeeld niet voldaan aan informatieplicht
Op een bedrijventerrein vindt cameratoezicht plaats. Bij de ingang van het bedrijventerrein hangt een duidelijk bord met een symbool van een camera. Dit bord met enkel een symbool is in dit geval niet voldoende, omdat het voor de bezoekers van het bedrijventerrein niet duidelijk is wie de verantwoordelijke is. Op het bord had derhalve de naam van de verantwoordelijke moeten worden vermeld.

[59] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 156.
[60] Zie voor de vraag of heimelijk cameratoezicht is toegestaan paragraaf 2.7 'Noodzakelijkheid, proportionaliteit en subsidiariteit'.
[61] Cameratoezicht dat niet op een duidelijke wijze kenbaar is gemaakt is onder omstandigheden strafbaar op grond van artikel 139f, lid 1, en 441b Wetboek van Strafrecht. Het vooraf informeren van alle werknemers over de mogelijke inzet van heimelijk cameratoezicht, neemt deze strafbaarheid weg.
[62] De Wet op de ondernemingsraden bepaalt dat de ondernemingsraad een instemmingsrecht heeft over een besluit om gebruik te maken van een personeelsvolgsysteem, waaronder een (verborgen) camera kan vallen (artikel 27).

Voorbeeld informeren na afloop heimelijk cameratoezicht
Een transportonderneming heeft een redelijk vermoeden dat een werknemer geregeld diefstal pleegt van lading uit een vrachtwagen wanneer hij de lading vervoert. De onderneming stelt heimelijk cameratoezicht in ten aanzien van de vrachtwagen waarin en de tijdstippen waarop de betreffende werknemer de lading vervoert. Daarbij komen zowel andere werknemers in beeld die helpen de lading te laden en lossen, als willekeurige voorbijgangers. Na afloop van het toezicht moet de onderneming álle werknemers die in beeld zijn gebracht informeren over de inzet van de heimelijke camera's. De onderneming kan evenwel niet achterhalen wie de willekeurige voorbijgangers zijn. Het zou onmogelijk zijn of in ieder geval een onevenredige inspanning kosten om deze voorbijgangers ook op de hoogte te stellen. De onderneming hoeft daarom in dit geval de voorbijgangers niet te informeren. Wel moet de onderneming de herkomst van de camerabeelden vastleggen.
Overigens mogen de camerabeelden niet langer worden bewaard dan noodzakelijk is voor het doel.[1] Wanneer de beelden dus niet of niet meer noodzakelijk zijn om de kwestie met betrekking tot de diefstal af te handelen, moet de onderneming de beelden onmiddellijk vernietigen.

1 Zie over het onderwerp bewaartermijnen paragraaf 2.9 'Bewaartermijn'.

3. Uitwerking artikel 151c Gemeentewet jo Wpg

Dit hoofdstuk bevat een uitwerking van artikel 151c Gemeentewet en bepalingen van de Wet politiegegevens (Wpg) die een belangrijke rol spelen bij de verwerking van persoonsgegevens door middel van cameratoezicht op openbare plaatsen[63] door gemeenten in het belang van de handhaving van de openbare orde. De terminologie en systematiek hiervan sluiten nauw aan bij de Wbp. De opbouw van dit hoofdstuk is daarom hetzelfde als van het vorige hoofdstuk. Paragraaf 3.1 tot en met 3.4 hebben betrekking op een aantal algemene begrippen. Paragraaf 3.5 tot en met 3.13 lichten een aantal inhoudelijke normen toe dat de verantwoordelijke moet naleven.

3.1 Politiegegevens

De persoonsgegevens die worden verwerkt door middel van het cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde zijn politiegegevens in de zin van de Wpg (artikel 151c, lid 9, Gemeentewet). In deze paragraaf wordt nader uitgewerkt wat onder het begrip 'politiegegevens' wordt verstaan.

Onder 'politiegegeven' wordt verstaan elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, sub a, Wpg). Het begrip 'persoonsgegeven' maakt dus onderdeel uit van het begrip 'politiegegeven'.

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1, sub a, Wbp).[64]

'Geïdentificeerde of identificeerbare'

Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.[65] Er kan een onderscheid worden gemaakt in direct en indirect identificeerbare gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificeerbare gegevens is sprake wanneer zij via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.[66] Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.[67]

Ingeval van cameratoezicht zal meestal sprake zijn van persoonsgegevens, aangezien personen vaak herkenbaar in beeld worden gebracht. Maar ook ingeval personen niet of niet herkenbaar in beeld worden gebracht, kan sprake zijn van persoonsgegevens, zolang de beelden betrekking hebben op een natuurlijke persoon en die persoon *identificeerbaar* is.

63 Onder 'openbare plaats' wordt verstaan een plaats die krachtens bestemming of vast gebruik openstaat voor het publiek (artikel 151c, lid 1, Gemeentewet j° artikel 1, lid 1, Wet openbare manifestaties). Dat de plaats openstaat voor het publiek wil zeggen dat in beginsel een ieder vrij is om er te komen, te vertoeven en te gaan. Dit betekent dat er geen beletselen in de vorm van een meldingsplicht, de eisen van voorafgaand verlof of de heffing van een toegangsbewijs gelden voor het betreden van de plaats. Kamerstukken II, 2003/04, 29 440, nr. 3, p. 8.
64 Zie voor meer informatie over dit onderwerp WP29, Advies 4/2007 over het begrip persoonsgegeven, WP136, 20 juni 2007.
65 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.
66 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48.
67 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.

Voorbeeld persoonsgegevens
In een uitgaansgebied worden video-opnames gemaakt ter handhaving van de openbare orde. Er is hier sprake van persoonsgegevens, aangezien de personen in het uitgaansgebied herkenbaar in beeld worden gebracht.

3.2 Verwerking

De persoonsgegevens die in het kader van artikel 151c Gemeentewet worden verwerkt zijn politiegegevens. Op de verwerking van politiegegevens is de Wpg van toepassing. Artikel 151c Gemeentewet en de Wpg kunnen dus alleen van toepassing zijn als sprake is van een geheel of gedeeltelijke geautomatiseerde verwerking van politiegegevens alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. In deze paragraaf wordt nader uitgewerkt wat onder het begrip 'verwerking' wordt verstaan.

De definitie van het begrip 'verwerking' in de Wpg is nagenoeg gelijkluidend aan de definitie in de Wbp. De Wpg bepaalt dat een verwerking van politiegegevens elke handeling of elk geheel van handelingen met betrekking tot politiegegevens betreft. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub c, Wpg).

Bij digitale camera's worden intern geheugen en een digitale processor gebruikt om de beeldgegevens op te slaan en door te zetten tussen verschillende componenten van het systeem. Dit betekent dat dit proces – hoe tijdelijk ook van karakter – altijd wordt beschouwd als een verwerking in de zin van de Wpg. Het actief gebruik van opnamefunctionaliteiten is niet relevant om te bepalen of er sprake zal zijn van een verwerking in de zin van de Wpg. Dit betekent dat er bij het gebruik van een digitale camera altijd een verwerking van persoonsgegevens plaatsvindt, ook als beelden niet actief worden vastgelegd. Daarmee is het live uitkijken middels een digitale camera een verwerking van persoonsgegevens en is de Wpg van toepassing.[68]

Voorbeeld verwerking
Een gemeente heeft op het stationsplein cameratoezicht ingesteld ter handhaving van de openbare orde. De digitale camerabeelden worden niet vastgelegd, maar live uitgekeken door de politie. Deze handeling – het live uitkijken van de digitale camerabeelden- is een verwerking van politiegegevens.

3.3 Verantwoordelijke

De verantwoordelijke voor de inzet van het cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde, is de burgemeester. De burgemeester bedient zich bij de uitvoering van het cameratoezicht evenwel van de onder zijn gezag staande politie (artikel 151c, lid 4, Gemeentewet). De politie voert de operationele regie en is daarvoor verantwoordelijk.[69] Meer specifiek geldt dat de korpschef de verantwoordelijke bij de politie is (artikel 1, sub f, onder 1, Wpg).

3.4 Bewerker[70]

Zoals in de vorige paragraaf 3.3 'Verantwoordelijke' reeds is vermeld, voert de politie de operationele regie ten aanzien van cameratoezicht dat is ingezet op grond van artikel 151c Gemeentewet. De politie kan bij het uitkijken van deze camerabeelden gebruik maken van een bewerker. Het besluit om op te treden naar aanleiding van waargenomen camerabeelden kan echter alleen worden genomen door de politie zelf en dus niet door de bewerker.

De definitie van het begrip 'bewerker' in de Wpg (artikel 1, sub i) is gelijkluidend aan de definitie in de Wbp.

De Wbp bepaalt dat de bewerker degene is die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1, sub e, Wbp).

---

[68] Voorheen was door het gebruik van analoge camera's geen sprake van een verwerking van persoonsgegevens, doordat de analoge camera's niet voorzien waren van digitale processoren. Tegenwoordig zijn bij de digitale camera's die in de omloop zijn deze standaard voorzien van digitale processoren, waardoor reeds daarom sprake is van verwerking van persoonsgegevens.
[69] *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 20 en *Kamerstukken II* 2004/05, 29 440, nr. 6, p.20 en 21.
[70] Zie voor meer informatie over dit onderwerp WP29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', WP169, 16 februari 2010.

De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon of instelling. Het zal veelal gaan om een persoon of instelling die niet in een hiërarchische relatie tot de verantwoordelijke staat. Daar waar een hiërarchische relatie bestaat met de verantwoordelijke moet worden gesproken van (intern) beheer. Tevens geldt dat de bewerker gegevens verwerkt ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. Voorts beperkt de bewerker zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt dus geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag van de gegevens enzovoorts.[71]

De verantwoordelijke die persoonsgegevens wil laten verwerken door een bewerker moet een overeenkomst met de bewerker sluiten waarin de uitvoering van de verwerkingen wordt geregeld (artikel 14, lid 2, Wbp). Dit vereiste van een bewerkersovereenkomst is in de Wpg van overeenkomstige toepassing verklaard (artikel 4, lid 6, Wpg).

Voorbeeld bewerker
Een gemeente heeft cameratoezicht ingesteld ter handhaving van de openbare orde. De politie heeft de regierol met betrekking tot de camerabeelden. Gelet op de beperkte politiecapaciteit laat de politie de beelden uitkijken door beveiligingsbeambten. Deze beveiligingsbeambten kunnen worden aangemerkt als bewerkers, waarmee een bewerkersovereenkomst moet worden afgesloten. De beveiligingsbeambten geven incidenten door aan de politie, zodat de politie kan beoordelen en beslissen om op te treden.

3.5 Doeleinden

Ten aanzien van cameratoezicht in het kader van artikel 151c Gemeentewet geldt een expliciete en begrensde doelbinding: de beelden mogen in het belang van de handhaving van de openbare orde in het kader van het toezicht op een openbare plaats worden verwerkt (artikel 151c, lid 8 j° lid 1, Gemeentewet). Hieronder valt zowel de daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde, alsook de algemene bestuurlijke voorkoming van strafbare feiten die invloed hebben op de orde en rust in de gemeentelijke samenleving.[72]

3.6 Grondslag

De grondslag voor het verwerken van persoonsgegevens door middel van cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde, zijn artikel 151c Gemeentewet, de betreffende verordening van de gemeenteraad en het betreffende besluit van de burgemeester. De burgemeester kan pas besluiten tot inzet van dit cameratoezicht indien de gemeenteraad hem bij verordening daartoe de bevoegdheid heeft verleend. Daarbij kan de gemeenteraad bepalen tot welke openbare plaatsen de bevoegdheid van de burgemeester zich uitstrekt en voor welke duur de plaatsing van camera's ten hoogste mag geschieden. De burgemeester besluit binnen welk gebied het cameratoezicht plaatsvindt en voor welke duur de gebiedsaanwijzing geldt binnen de marges van de verordening (artikel 151c, lid 1 en 2, Gemeentewet).

Deze wettelijke grondslag betreft een discretionaire bevoegdheid. Het schept dus geen verplichting voor gemeenten om cameratoezicht toe te passen.

Voorbeeld geen grondslag
Een gemeente wil cameratoezicht instellen ter handhaving van de openbare orde. De gemeenteraad heeft de burgemeester hiertoe echter niet bij verordening de bevoegdheid gegeven. De burgemeester heeft daarom geen grondslag voor de verwerking van persoonsgegevens bij de inzet van het cameratoezicht.

Voorbeeld onjuiste grondslag
Een gemeente filmt de ingang van het gemeentehuis ter beveiliging van haar bezoekers en gebouw. De grondslag voor dit cameratoezicht baseert de gemeente op artikel 151c Gemeentewet. Op grond van dit artikel mag echter alleen cameratoezicht worden ingezet op openbare plaatsen ter handhaving van de openbare orde en niet ter beveiliging van eigen gebouwen en de bezoekers daarvan. De gemeente heeft daarom het cameratoezicht gebaseerd op een onjuiste grondslag. Als mogelijke grondslag zou wel kunnen gelden het 'gerechtvaardigd belang' als bedoeld in artikel 8, sub f, Wbp.[1]

[1] Zie over de grondslagen genoemd in artikel 8 Wbp paragraaf 2.6 'Grondslagen'.

[71] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 61.
[72] *Kamerstukken II* 1989/90, 19 403, nr. 16, p. 38, *Kamerstukken II* 2003/04, 29 440, nr. 3, p. 6 en 9 en *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 4–5.

3.7 Noodzakelijkheid, proportionaliteit en subsidiariteit

Een belangrijk vereiste van een gerechtvaardigde verwerking van persoonsgegevens door middel van cameratoezicht op basis van artikel 151c Gemeentewet betreft de noodzakelijkheid van de verwerking. Cameratoezicht mag namelijk pas worden ingezet indien dat in het belang van de handhaving van de openbare orde *noodzakelijk* is (artikel 151c, lid 1, Gemeentewet). Hierbij spelen de beginselen van proportionaliteit en subsidiariteit een belangrijke rol.

Het proportionaliteitsbeginsel houdt in dat de inbreuken op de belangen van de betrokkenen niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel.[73] Ingevolge het subsidiariteitsbeginsel moet het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de betrokkenen minder nadelige, wijze kunnen worden verwerkelijkt.[74]

Concreet betekent dit dat telkens nauwkeurig zal moeten worden afgewogen welke openbare plaatsen wel, en welke niet, worden aangewezen voor cameratoezicht. Een enkele en ongemotiveerde verwijzing naar de gehele binnenstad geeft geen blijk van een dergelijke zorgvuldige afweging.[75] Cameratoezicht kan immers alleen worden ingezet in gebieden waar er een bovengemiddeld risico bestaat op verstoringen van de openbare orde.[76] Daarbij baseert de burgemeester zich op informatie van de politie. Deze informatie geeft de burgemeester een beeld van de veiligheidssituatie van een gebied. Ook kan de burgemeester zich baseren op de zogenoemde Integrale Veiligheidsmonitor.[77] Ook brengt dit met zich mee dat cameratoezicht ter handhaving van de openbare orde slechts mag worden ingezet indien ook andere maatregelen zijn getroffen.[78] Minder vergaande maatregelen moeten onvoldoende effectief zijn en deze maatregelen kunnen redelijkerwijs niet worden uitgebreid. Tevens mogen niet meer en langer camera's worden ingezet en niet meer personen en/of plaatsen in beeld worden gebracht dan strikt noodzakelijk is voor de gestelde doeleinden (dataminimalisatie). Dit betekent dat de gemeente alleen continu cameratoezicht mag instellen wanneer niet kan worden volstaan met opnames gedurende bepaalde periodes. Bovendien mag door de camera's niet meer van de openbare ruimte worden bestreken dan het gebied dat door de gemeenteraad en de burgemeester expliciet is aangewezen. Het is niet toegestaan dat camera's video-opnames maken van privévertrekken, zoals van tuinen en het interieur van woonhuizen, of op andere wijze een ongerechtvaardigde inbreuk maken op de privésfeer van burgers.[79]

Cameratoezicht in een openbaar toilet maakt een te grote inbreuk op de persoonlijke levenssferen van de betrokkenen. Cameratoezicht in deze ruimte voldoet daarmee niet aan het vereiste van proportionaliteit en is dus niet toegestaan.

Voorts geldt dat het plaatsen van camerabeelden op internet vaak niet noodzakelijk is. De belangen van de betrokkenen kunnen hierdoor immers onevenredig worden geschaad doordat de beelden voor een ieder toegankelijk zijn (disproportioneel).

De noodzaak van de gegevensverwerking moet aanwezig zijn gedurende het gehele verwerkingsproces en dus niet slechts op het moment dat de verwerking begint. Artikel 151c Gemeentewet bepaalt expliciet dat de burgemeester het besluit tot cameratoezicht intrekt zodra de inzet van camera's niet langer noodzakelijk is in het belang van de handhaving van de openbare orde (lid 5). Dit betekent dat de burgemeester zich regelmatig ervan moet vergewissen of het cameratoezicht nog steeds noodzakelijk is.[80] Wat 'regelmatig' is, is afhankelijk van de omstandigheden van het concrete geval. Factoren die hierbij een rol kunnen spelen zijn onder meer de ernst van de situatie waarvoor en de omgeving waarbinnen het cameratoezicht wordt ingesteld en eventuele veranderingen van de omstandigheden.

Heimelijk cameratoezicht

Heimelijk cameratoezicht op grond van artikel 151c Gemeentewet is *niet* toegestaan. De aanwezigheid van camera's moet op duidelijke wijze kenbaar zijn voor een ieder die het betreffende gebied betreedt

---

[73] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 8.
[74] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 8–9.
[75] *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 14 en nr. 6, p. 15.
[76] *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 1.
[77] De Integrale Veiligheidsmonitor is een bevolkingsonderzoek naar veiligheid, leefbaarheid en slachtofferschap dat gemeenten een beeld geeft van de veiligheidsbeleving van hun inwoners en hun wensen en behoeften op het gebied van veiligheid. *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 13–14 en 18 en *Kamerstukken I* 2014/15, 33 582, B, p. 8.
[78] Zie ook *Kamerstukken II* 2003/04, 29 440, nr. 3, p. 11, *Kamerstukken II* 2004/05, 29 440, nr. 66, p. 4227 en 4228 en *Kamerstukken II* 2004/05, 29 440, nr. 30, p. 1434.
[79] Zie ook *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 14 en 15 en *Kamerstukken II* 2003/04, 29 440, nr. 3, p. 11–12.
[80] Zie ook *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 5–6 en nr. 6, p. 23.

(artikel 151c, lid 6, Gemeentewet). De camera's zelf hoeven echter niet zichtbaar te zijn.[81]

Voorbeeld noodzakelijk
In een uitgaansgebied vinden 's nachts in het weekend vaak ongeregeldheden plaats. De betreffende gemeente heeft reeds extra verlichting aangebracht en de politie surveilleert vaker. Deze maatregelen blijken echter onvoldoende effect te sorteren, waardoor de gemeente heeft besloten tot het inzetten van cameratoezicht. De camera's staan alleen aan gedurende de nachtelijke uren in het weekend. De gemeente heeft hiermee de noodzaak (proportionaliteit en subsidiariteit) van het cameratoezicht aangetoond.

Voorbeeld niet langer noodzakelijk
Sinds de opening van een discotheek vinden er geregeld ongeregeldheden plaats. De betreffende gemeente besluit uiteindelijk tot de inzet van cameratoezicht voor een bepaalde tijdsduur ter handhaving van de openbare orde. Voordat deze tijdsduur afloopt, sluit de discotheek voorgoed zijn deuren. Ondanks dat de bepaalde tijdsduur voor het cameratoezicht nog niet is verstreken, moet de gemeente zich ervan vergewissen of het cameratoezicht nog noodzakelijk is, nu de discotheek is gesloten (verandering van omstandigheden).

3.8 Verdere verwerking

In het algemeen geldt dat persoonsgegevens alleen verder mogen worden verwerkt op een wijze die niet onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Artikel 151c, lid 9, Gemeentewet bevat hierop een uitzondering: de camerabeelden die in het belang van de handhaving van de openbare orde zijn verzameld, mogen worden verwerkt ten behoeve van de opsporing van een concreet strafbaar feit.

Deze gegevensverstrekking zal uitsluitend mogen plaatsvinden indien een concrete aanleiding bestaat voor de veronderstelling dat op de beelden gegevens staan die noodzakelijk[82] zijn voor de opsporing van een gepleegd strafbaar feit. Dit betekent dat sprake moet zijn van aanwijzingen dat de opnames die zijn verkregen door middel van cameratoezicht relevant materiaal bevatten. Deze uitzonderingsgrond beperkt zich niet tot persoonsgegevens waaruit een gegeven van een strafbaar feit blijkt. Het beperkt zich evenmin tot verdachten maar kan ook betrekking hebben op het opsporen van getuigen.[83]

Voorbeeld onverenigbaar
Een gemeente heeft video-opnames gemaakt van haar centrum ter handhaving van de openbare orde. De gemeente wil de video-opnames gebruiken voor het online promoten van de gemeente om toeristen aan te trekken. Het gebruik van de video-opnames voor het nieuwe doel (het online promoten van de gemeente) is onverenigbaar met het oorspronkelijke doel van het cameratoezicht (de handhaving van de openbare orde). Het verdere gebruik van de video-opnames is in dit geval dus niet gerechtvaardigd.

3.9 Bewaartermijn

Ten aanzien van het verwerken van persoonsgegevens door middel van cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde, geldt een wettelijke bewaartermijn van *maximaal* vier weken (artikel 151c, lid 9, Gemeentewet).

Indien deze persoonsgegevens verder worden verwerkt ten behoeve van de opsporing van een concreet strafbaar feit, dan wordt de duur van de opslag bepaald door dit nieuwe doel.[84]

3.10 Beveiliging[85]

De persoonsgegevens die in het kader van artikel 151c Gemeentewet worden verwerkt zijn politiegegevens. Op de verwerking van politiegegevens is de Wpg van toepassing. Op grond van de Wpg moet de politie de camerabeelden van de openbare plaatsen adequaat beveiligen. Artikel 4, lid 3, Wpg vereist dat de politie passende technische en organisatorische maatregelen treft om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via directe geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveili-

[81] *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 15.
[82] Zie over het begrip noodzakelijkheid en de invulling daarvan paragraaf 3.7 'Noodzakelijkheid, proportionaliteit en subsidiariteit'.
[83] *Kamerstukken II* 2003/04, 29 440, nr. 3, p. 13 en 18.
[84] De beelden mogen dan worden verwerkt totdat ze niet meer nodig zijn voor opheldering, vervolging en berechting van het strafbare feit. In de Wpg worden deze termijnen nader gespecificeerd.
[85] Zie voor meer informatie over dit onderwerp de CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013.

gingsniveau, gelet op de risico's van de verwerking en de aard van de politiegegevens.

Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act cyclus in de dagelijkse praktijk van de organisatie noodzakelijk.[86]

Een onderdeel van de benodigde beveiliging is het voorkomen dat onbevoegden toegang kunnen krijgen tot de camerabeelden. Welke personen er toegang mogen krijgen (geautoriseerd zijn) is afhankelijk van de functie die zij bekleden alsmede van de aard van de gegevens en de doeleinden van het cameratoezicht. Hieronder kunnen ook de mensen vallen die onderhoudswerkzaamheden aan de camera-installatie verrichten. De activiteiten die deze personen met de camerabeelden uitvoeren alsmede pogingen van anderen om ongeautoriseerd toegang te krijgen, moeten worden gelogd.[87] Het uitvoeren van een PIA[88] kan de verantwoordelijke helpen om te bepalen welke beveiligingsmaatregelen noodzakelijk zijn.

3.11 Gevoelige politiegegevens

De Wpg noemt in artikel 5 politiegegevens die als gevoelig worden aangemerkt. Het betreft de politiegegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging. De verwerking van deze gevoelige politiegegevens mag alleen plaatsvinden in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

3.12 Melden

Er geldt geen plicht om de voorgenomen verwerking van persoonsgegevens door middel van cameratoezicht op grond van artikel 151c Gemeentewet te melden bij de Autoriteit Persoonsgegevens.[89]

3.13 Informeren betrokkenen

De aanwezigheid van cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde moet op een duidelijke wijze kenbaar zijn voor een ieder die de desbetreffende openbare plaats betreedt (artikel 151c, lid 6, Gemeentewet).[90] Dit betekent dat niet kan worden volstaan met het plaatsen van één bord op een centrale plek binnen het cameragebied. Aan de betrokkenen moet in ieder geval aan de randen van het cameragebied kenbaar worden gemaakt dat zij een cameragebied betreden.[91] De camera's zelf hoeven echter niet zichtbaar te zijn. Ook hoeft niet zichtbaar te zijn of de camera's in werking zijn.[92]

Voorts geldt dat aan het vereiste van kenbaarheid niet alleen moet worden voldaan als er beelden worden vastgelegd, maar ook als sprake is van monitoring en er dus geen opnames worden gemaakt.[93]

4. Cameratoezicht op combinatie van private goederen en openbare plaatsen

In de hoofdstukken 2 en 3 zijn bepalingen ten aanzien van – kort weergegeven – privaat cameratoezicht (Wbp) en gemeentelijk cameratoezicht (artikel 151c Gemeentewet j° Wpg) gescheiden van elkaar weergegeven. In het algemeen geldt hierbij dat de video-opnames door private organisaties niet verder mogen reiken dan tot hetgeen onder hun eigen verantwoordelijkheid valt[94] en de videoopnames door gemeenten niet verder mogen reiken dan openbare plaatsen. Er kunnen zich echter situaties voordoen waarin private organisaties eveneens delen van openbare plaatsen filmen of waarin private organisaties en gemeenten gezamenlijk zowel private goederen als openbare plaatsen filmen. Dit hoofdstuk gaat nader in op deze situaties.

---

[86] CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 14 e.v.
[87] CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22.
[88] Zie over het onderwerp PIA ook Hoofdstuk '1. Algemene uitgangspunten verwerking persoonsgegevens door middel van camera's'.
[89] Ingevolge artikel 38 lid 2 van het Vrijstellingsbesluit van de Wbp.
[90] Overigens moet ook de gebiedsaanwijzing van de burgemeester op behoorlijke wijze kenbaar worden gemaakt. Dit besluit moet worden bekendgemaakt door kennisgeving van het besluit of van de zakelijke inhoud ervan in een van overheidswege uitgegeven blad of een dag-, nieuws- of huis-aan-huisblad, dan wel op een andere geschikte wijze (artikel 3:42 Algemene wet bestuursrecht). Als een gebiedsaanwijzing wordt ingetrokken, moet ook dat besluit bekend worden gemaakt (artikel 3:42, lid 2, Algemene wet bestuursrecht). Zie *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 12.
[91] *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 12.
[92] *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 15.
[93] *Kamerstukken II* 2003/04, 29 440, nr. 3, p. 17 en zie ook paragraaf 3.2 van deze beleidsregels.
[94] Zoals bij de beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen (artikel 38 Vrijstellingsbesluit).

4.1 Video-opnames van openbare plaatsen door private organisaties

Cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde is uitsluitend voorbehouden aan gemeenten op grond van artikel 151c Gemeentewet. Dit neemt evenwel niet weg dat private organisaties soms ook delen van openbare plaatsen filmen. Private organisaties zijn hiertoe slechts gerechtigd voor zover het in beeld brengen van deze delen van de openbare ruimte *onvermijdelijk* is ter beveiliging van personen en goederen die aan hun zorg zijn toevertrouwd.[95]

Op dit cameratoezicht door private organisaties is de Wbp van toepassing. Zie voor een uitwerking van bepalingen van de Wbp hoofdstuk 2 '*Uitwerking Wbp*' in aanvulling daarop geldt dat het doeleinde van dit cameratoezicht door private organisaties, waarbij delen van openbare plaatsen in beeld worden gebracht, er niet op mag zijn gericht om toezicht te houden op die openbare plaatsen. Voor dit doeleinde zijn immers de gemeenten verantwoordelijk. Als gerechtvaardigd doeleinde kan wel worden aangemerkt de beveiliging van de personen en goederen die aan de zorg van de betreffende private organisaties zijn toevertrouwd. De private organisaties zijn verantwoordelijk voor de verwerking van persoonsgegevens die voor dit doeleinde worden verwerkt. Voorts geldt dat geen grotere delen van de openbare plaatsen in beeld mogen worden gebracht voor zover dat noodzakelijk is om dit doeleinde te bereiken.

Verantwoordelijkheid gemeenten

De burgemeester is belast met de handhaving van de openbare orde (artikel 172, lid 1, Gemeentewet). Ook indien private organisaties cameratoezicht hebben ingesteld op delen van openbare plaatsen, blijft de burgemeester verantwoordelijk voor de handhaving van de openbare orde op deze plaatsen.

Op welke wijze de burgemeester invulling kan geven aan zijn verantwoordelijkheid, is afhankelijk van de situatie. Zo is het mogelijk dat de burgemeester (camera)toezicht instelt op de openbare plaatsen die mede door de private organisaties worden gefilmd. Een ander voorbeeld is dat de burgemeester eisen stelt aan de reikwijdte van het cameratoezicht op de openbare plaatsen door private organisaties of aan de wijze waarop betrokkenen over dit cameratoezicht moeten worden geïnformeerd.

Voorts geldt dat de burgemeester bevoegd is om overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde, te beletten of te beëindigen (artikel 172, lid 2, Gemeentewet). Zo kan de burgemeester optreden ingeval de bepalingen van een Algemene Plaatselijke Verordening worden overtreden door de inzet van het cameratoezicht door private organisaties.

Voorbeeld niet onvermijdelijk
Een avondsupermarkt filmt de openbare weg grenzend aan de winkel, omdat daar vaak geluidsoverlast plaatsvindt door uitgaande jongeren. De avondsupermarkt wil deze beelden verstrekken aan de politie en de gemeente zodat zij maatregelen gaan treffen tegen de overlast. De handhaving van de openbare orde is echter voorbehouden aan de gemeente. De avondsupermarkt heeft niet aangetoond dat het cameratoezicht onvermijdelijk is ter beveiliging van personen en goederen die aan zijn zorg zijn toevertrouwd. Dit cameratoezicht is derhalve ongeoorloofd.

Voorbeeld niet onvermijdelijk
Een supermarkt heeft bij de ingang van de winkel een camera geplaatst tegen winkeldiefstal. De camera filmt de openbare weg. De supermarkt heeft niet aangetoond waarom video-opnames van alleen de winkel, zoals van de schappen en de kassa's, onvoldoende effectief is tegen winkeldiefstal. Er is in dit geval geen sprake van een noodzaak om de openbare weg te filmen, zodat dit cameratoezicht ongeoorloofd is.

Voorbeeld onvermijdelijk
Een juwelier heeft bij de ingang van de winkel een camera geplaatst tegen beroving. De camera filmt een klein gedeelte van de openbare weg dat direct aan de ingang van de winkel grenst. Dit gedeelte van de openbare weg wordt gefilmd, omdat is gebleken dat overvallers zich vlak voor de winkel vermommen voordat ze de winkel betreden. De juwelier heeft aangetoond dat het onvermijdelijk is om een dit kleine gedeelte van de openbare weg te filmen om zijn zaak goed te kunnen beveiligen. Dit cameratoezicht is derhalve geoorloofd.

[95] Toelichting op het Vrijstellingsbesluit Wbp, Stb. 2001, 250, p. 72.

Voorbeeld verantwoordelijke private organisatie
De beveiliging van een bedrijventerrein is in handen van een stichting. Deze stichting heeft camera's opgehangen ter beveiliging van haar bedrijventerrein. De betreffende gemeente en de stichting hebben aangegeven dat de stichting verantwoordelijk is voor het cameratoezicht op het bedrijventerrein. Er is geen besluit in de zin van artikel 151c Gemeentewet genomen, omdat het doel van het cameratoezicht niet de handhaving van de openbare orde betreft, maar uitsluitend de beveiliging van private eigendommen en de openbare weg wordt ook *niet* in beeld gebracht. Het cameratoezicht valt volgens beide partijen buiten de reikwijdte van artikel 151c Gemeentewet, omdat er geen sprake is van wanordelijkheden die de openbare orde verstoren, zoals samenscholing, geluidsoverlast, scheld- en vechtpartijen, bedreigende taal en vandalisme. In dit geval is het regime van de Wbp van toepassing op het ingestelde cameratoezicht. De verantwoordelijke in de zin van de Wbp voor het cameratoezicht op het bedrijventerrein is de stichting.

Voorbeeld publiek-private samenwerking
De beveiliging van een bedrijventerrein is in handen van een stichting. Deze stichting heeft camera's opgehangen ter beveiliging van haar bedrijventerrein. De camera's filmen ook de openbare weg die grenst aan het bedrijventerrein. In dit geval is het regime van de Wbp van toepassing op het ingestelde cameratoezicht. De verantwoordelijke in de zin van de Wbp voor het cameratoezicht op het bedrijventerrein is de stichting. Ook onder het Wbp-regime kan de betreffende gemeente zich echter niet onttrekken aan haar verantwoordelijkheid voor de openbare weg die in beeld wordt gebracht. De gemeente is een vaste deelnemer bij de overleggen van de stichting en maakt onderdeel uit van het bestuur van de stichting. Deze gemeentelijke invloed is schriftelijk vastgelegd in de statuten van de stichting. De verantwoordelijkheid van de gemeente lijkt in deze situatie voldoende te zijn gewaarborgd.

Voorbeeld publiek-private samenwerking
Een eigenaar van een bedrijventerrein heeft camera's opgehangen ter beveiliging van het terrein. De camera's filmen ook de openbare weg die grenst aan het bedrijventerrein. Het cameratoezicht valt onder de Wbp en de eigenaar van het terrein is de verantwoordelijke. De eigenaar en de betreffende gemeente hebben een convenant gesloten waarin het doel en de voorwaarden van het cameratoezicht op de openbare weg schriftelijk zijn vastgelegd. Een betrokkene klaagt vervolgens dat een te groot deel van de openbare weg wordt gefilmd (niet noodzakelijk in de zin van artikel 8 Wbp[1]). De eigenaar wijst de klacht af met een verwijzing naar het convenant waarin de gemeente de voorwaarden van het cameratoezicht op de openbare weg heeft 'goedgekeurd'. De eigenaar heeft hiermee de klacht op onjuiste gronden afgewezen. Een convenant kan immers helderheid verschaffen over de wijze waarop partijen invulling geven aan de wettelijke normen, maar vervangt die normen niet. De eigenaar blijft verantwoordelijke in de zin van de Wbp voor de naleving van de Wbp en kan deze verantwoordelijkheid niet afschuiven op de gemeente. De eigenaar had daarom de reikwijdte van het cameratoezicht moeten toetsen aan de Wbp.

[1] Zie over het noodzakelijkheidsvereiste in de zin van artikel 8 Wbp paragraaf 3.7 'Noodzakelijkheid, proportionaliteit en subsidiariteit'.

4.2 Video-opnames van private goederen en openbare plaatsen door private organisaties en gemeenten

Tegenwoordig komt het steeds vaker voor dat private organisaties en gemeenten en/of politie samenwerken bij de inzet van cameratoezicht. Zo kunnen partijen afspreken en faciliteren wanneer en op welke wijze (live) camerabeelden worden verstrekt aan de politie.[96] Tevens kunnen private partijen en gemeenten gebruik maken van dezelfde camera's. De camera's filmen dan zowel private goederen als openbare plaatsen ten behoeve van twee verschillende doeleinden: de beveiliging van de private goederen alsmede de handhaving van de openbare orde.

Ten aanzien van deze samenwerkingsvormen gelden twee verschillende wettelijke kaders. Enerzijds gelden de vereisten van de Wbp ten aanzien van de beveiliging van private goederen door private organisaties. Anderzijds gelden de vereisten van artikel 151c Gemeentewet ten aanzien van de handhaving van de openbare orde door gemeenten. Beide partijen moeten voldoen aan de voor hen geldende vereisten. Om dit te waarborgen, is het van belang dat partijen, voorafgaand aan het inzetten van gezamenlijk cameratoezicht, schriftelijk heldere en werkbare afspraken maken.[97]

Zie voor een uitwerking van vereisten van de wettelijke kaders de vorige hoofdstukken 2 'Uitwerking Wbp' en 3 'Uitwerking artikel 151c Gemeentewet j° Wpg'. In aanvulling op deze uitwerkingen wordt nog het volgende benadrukt.

Er kan slechts gebruik worden gemaakt van dezelfde camera's *voor zover* de private partijen gerechtigd zijn om de betreffende delen van de openbare plaatsen te filmen en de gemeenten gerechtigd zijn om de betreffende private goederen in beeld te brengen. Dit betekent bovendien dat, zodra bij één van de partijen geen sprake meer is van een noodzaak tot cameratoezicht, deze partij de betreffende camerabeelden niet meer mag verwerken. De andere partij mag de camerabeelden dan nog wel

[96] De politie voert de operationele regie bij cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde.
[97] Zie ook *Kamerstukken II* 2012/13, 33 582, nr. 6, p. 11.

blijven verwerken, mits de noodzaak van het cameratoezicht voor die andere partij nog wel aanwezig is.

Tevens is het van belang dat de opslag van de camerabeelden ten behoeve van de beveiliging van private goederen en ten behoeve van de handhaving van de openbare orde, gescheiden geschiedt. Alleen op deze wijze kunnen de verschillende partijen voldoen aan de op hen betrekking hebbende wettelijke vereisten. Immers, de vereisten met betrekking tot bijvoorbeeld verdere verwerking, bewaartermijnen en toegangsbeveiliging kunnen voor de diverse partijen verschillen.

Voorts moeten de private organisaties en de gemeenten erop bedacht zijn dat de inzet van gezamenlijke camera's implicaties kan hebben voor de wijze waarop betrokkenen moeten worden geïnformeerd over het cameratoezicht. Voor betrokkenen moet immers duidelijk zijn dat het toezicht plaatsvindt voor verschillende doeleinden en door verschillende verantwoordelijken. Eveneens moet duidelijk zijn in welk gebied het cameratoezicht plaatsvindt. De informatieverstrekking moet bovendien worden aangepast zodra één van de partijen stopt met de verwerking de camerabeelden.

Voorbeeld samenwerking met gerechtvaardigd belang
De stationshallen in gemeente Y zijn in particulier eigendom. De eigenaar van deze hallen wil cameratoezicht instellen ter beveiliging van personen en goederen die aan zijn zorg zijn toevertrouwd.
Voornoemde stationshallen zijn voor een ieder toegankelijk, zodat de hallen ook een openbare plaats zijn. De gemeente Y wil cameratoezicht instellen ter handhaving van de openbare orde in deze hallen.
Beide partijen voldoen aan de voor hen geldende wettelijke vereisten voor het inzetten van cameratoezicht. Ze besluiten om gebruik te maken van gezamenlijke camera's en maken hierover schriftelijke afspraken. Tevens slaan ze de camerabeelden gescheiden van elkaar op. De verwerking van persoonsgegevens door beide partijen is in dit geval geoorloofd.

Voorbeeld samenwerking met gerechtvaardigd belang
De zijgevel van bedrijf A is diverse malen met graffiti bespoten. Bedrijf A wil daartegen cameratoezicht instellen. De zijgevel grenst direct aan straat X, zijnde de openbare weg, zodat het onvermijdelijk is dat ook een deel van de openbare weg in beeld wordt gebracht.
In straat X, langs de zijgevel van bedrijf A, vindt vaak overlast plaats door hangjongeren. De gemeente wil daartegen cameratoezicht instellen. Straat X grenst direct aan de zijgevel van bedrijf A, zodat ook die zijgevel in beeld zal worden gebracht.
Beide partijen voldoen aan de voor hen geldende wettelijke vereisten voor het inzetten van cameratoezicht. Ze besluiten om gebruik te maken van gezamenlijke camera's en maken hierover schriftelijke afspraken. Op de camerabeelden zal de zijgevel van bedrijf A en een deel van straat X te zien zijn. Tevens slaan partijen de camerabeelden gescheiden van elkaar op. De verwerking van persoonsgegevens door beide partijen is in dit geval geoorloofd.

Voorbeeld samenwerking zonder gerechtvaardigd belang
De zijgevel van bedrijf A is diverse malen met graffiti bespoten. Bedrijf A wil daartegen cameratoezicht instellen. De zijgevel grenst direct aan straat X, zijnde de openbare weg, zodat het onvermijdelijk is dat ook een deel van de openbare weg in beeld wordt gebracht.
Op het grasveld, verderop gelegen aan straat X, vindt vaak overlast plaats door hangjongeren. De gemeente wil daartegen cameratoezicht instellen.
Partijen besluiten om gebruik te maken van gezamenlijke camera's. Op de camerabeelden zal de zijgevel van bedrijf A, de volledige straat X en het grasveld te zien zijn. Het is evenwel niet noodzakelijk dat bedrijf A beelden van de volledige straat X en het grasveld verwerkt ten behoeve van de beveiliging van zijn pand. Tevens is het niet noodzakelijk dat de gemeente beelden van de zijgevel van bedrijf A verwerkt ten behoeve van de handhaving van de openbare orde op het grasveld. Beide partijen voldoen daarom niet aan het noodzakelijkheidsvereiste, zodat deze samenwerking niet geoorloofd is.

5. Drones[98], dashcams en andere slimme camera's

In de voorafgaande hoofdstukken is gesproken over camera's in het algemeen. Er zijn echter verschillende soorten camera's en ook verschillende softwaretechnieken. Zo kunnen camera's statisch[99] of gemakkelijk verplaatsbaar zijn of mobiel, bijvoorbeeld doordat een camera is bevestigd aan een lichaam[100], auto[101] of drone. Camera's kunnen roteren, inzoomen of geluid opnemen. Door middel van infraroodcamera's kunnen opnames worden gemaakt in de duisternis of warmtebronnen zichtbaar worden gemaakt. En camera's kunnen 'slim' of 'intelligent' zijn, waardoor de camera's niet slechts 'waarnemen', maar ook informatie genereren.

Zoals ook in hoofdstuk 1 'Algemene uitgangspunten verwerking persoonsgegevens door middel van camera's' is aangegeven, zijn de toepasselijke wettelijke regelingen voor de verwerking van persoons-

---

98 Zie voor meer informatie over dit onderwerp WP29, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, WP231, 16 juni 2015. Hiermee wordt bedoeld dat de camera nagelvast is bevestigd, bijvoorbeeld door montage aan gevels, dakranden of palen.
99 Hiermee wordt bedoeld dat de camera nagelvast is bevestigd, bijvoorbeeld door montage aan gevels, dakranden of palen.
100 Ook wel bodycams genoemd.
101 Ook wel dashcams genoemd.

gegevens door middel van cameratoezicht afhankelijk van de vragen wie de verantwoordelijke is en voor welke doeleinden het cameratoezicht wordt ingesteld. Het soort camera of softwaresysteem dat hiervoor wordt gebruikt, heeft hierop geen invloed. Er bestaat geen aparte wetgeving voor bepaalde soorten camera's of softwaresystemen. Indien in een concrete situatie van toepassing, gelden de bepalingen uit de Wbp of artikel 151c Gemeentewet j° de Wpg dus onverkort. Relevante bepalingen van deze wettelijke regelingen zijn uitgewerkt in de hoofdstukken 2, 3 en 4 van deze beleidsregels.

Wel kan het soort camera of softwaresysteem invloed hebben op de vraag of de gegevensverwerking gerechtvaardigd is. De ene camera of softwaretechniek kan immers een grotere inbreuk op de persoonlijke levenssfeer maken dan de andere. Het is daarom van belang dat de verantwoordelijke zorgvuldig afweegt welk soort camera met welke softwaretechnieken hij *ingeval van cameratoezicht* inzet. Indien een camera of softwaretechniek een onevenredige inbeuk maakt op de belangen van de betrokkenen in verhouding tot het te dienen doel (proportionaliteit) of het doel ook op een andere, voor de betrokkenen minder nadelige, wijze kan worden verwezenlijkt (subsidiariteit), dan is de inzet van deze camera of softwaretechniek niet geoorloofd.

Drones en dashcams zijn voorbeelden van zich technisch snel ontwikkelende 'slimme' camera's, die steeds meer toepassing vinden.

Dit hoofdstuk gaat in paragraaf 5.1 nader in op cameratoezicht door middel van drones, in paragraaf 5.2 zal het gaan om dashcams en in paragraaf 5.3 gaat het over andere slimme camera's.

5.1 Drones[102]

Met het begrip 'drone' wordt bedoeld een onbemand luchtvaartuig. Andere begrippen die in dit kader ook vaak worden gebruikt zijn:
- Unmanned Aircraft (UA): een onbemand luchtvaartuig
- Unmanned Aerial Vehicle (UAV): een onbemand luchtvaarttoestel
- Unmanned Aircraft System (UAS): een onbemand luchtvaartuigsysteem
- Remotely Piloted Aircraft System (RPAS): een onbemand luchtvaartuigsysteem op afstand bestuurd (door een piloot).

In deze beleidsregels wordt evenwel als overkoepelende term de term 'drone' gehanteerd.[103]

Voor recreatief gebruik van drones (model) is geen vergunning nodig. Wel moet worden voldaan aan de bepalingen uit de Regeling modelvliegtuigen.[104] Deze Regeling modelvliegtuigen stelt regels omtrent het gebruik van het luchtruim. Hieronder vallen bijvoorbeeld regels omtrent de vlieghoogte en waar wel en niet mag worden gevlogen. Zo verbiedt de luchtvaartregelgeving[105] onder andere om boven gebieden met aaneengesloten bebouwing of boven mensenmenigten te vliegen. Behoudens een ontheffing mogen drones dus niet in de buurt komen van een woonwijk of van (andere) plaatsen waar zich mensenmenigten of doorgaans mensen bevinden. Bovendien kunnen lagere overheden extra regels stellen in verordeningen, bijvoorbeeld in het kader van milieu, openbare orde en veiligheid. Dit kan verschil maken ten aanzien van de inbreuk op de persoonlijke levenssfeer.

Voor drones die vanuit beroepsmatige of bedrijfsmatige overwegingen worden bediend, is respectievelijk een bewijs van bevoegdheid, een bewijs van luchtwaardigheid en een zogenoemde Remotely piloted aircraft system operator certificate (ROC) vereist.[106]

Drones kunnen worden uitgerust met (hoge resolutie) camera's. Hierdoor wordt het mogelijk om (gedetailleerde en ingezoomde) video-opnames te maken vanuit de lucht. Tevens wordt het mogelijk om video-opnames te maken van plaatsen die moeilijk of niet op andere wijzen kunnen worden gemaakt. Drones kunnen bovendien naar behoefte worden gestuurd en zijn in staat om in korte tijd grote afstanden af te leggen. Juist deze eigenschappen kunnen leiden tot een grote inbreuk op de persoonlijke levenssfeer.

---

[102] Voor de praktische toepassing van drones, zie: 'Handleiding Drones en Privacy' (Kamerstukken II 2015/16, 30 806, nr. 34).
[103] Strikt genomen is een drone echter een militair vliegtuig die autonoom een vooraf geprogrammeerde vliegbaan aflegt. Een RPAS is dus eigenlijk geen drone (http://www.darpas.nl/faq/).
[104] Regeling modelvliegen van de Staatssecretaris van Verkeer en Waterstaat van 2 december 2005, nr. HDJZ/LUV/2005-2297, Hoofddirectie Juridische Zaken, houdende nadere regels voor vluchten met een modelvliegtuig (Regeling modelvliegen).
[105] Zie: artikel 2 van de Regeling Modelvliegen juncto artikelen 14 en 15 van de Regeling op afstand bestuurde luchtvaartuigen.
[106] Deze regelgeving is uitgewerkt in het Besluit van 23 april 2015 tot wijziging van het Besluit bewijzen van bevoegdheid voor de luchtvaart, het Besluit luchtvaartuigen 2008, het Besluit vluchtuitvoering en het Besluit burgerluchthavens (regels voor op afstand bestuurde luchtvaartuigen), *Stb.* 2015, 163 alsmede in de Regeling van de Staatssecretaris van Infrastructuur en Milieu, van 23 april 2015, IENM/BSK-2015/11533, houdende de vaststelling van regels voor op afstand bestuurde luchtvaartuigen, *Stcrt.* 2015, nr. 12034.

Door middel van drones met camera's kunnen immers opnames worden gemaakt van personen op plaatsen waar zij verwachten onbespied te zijn. Te denken valt aan private terreinen of plaatsen waar geen mogelijkheden zijn om camera's te bevestigen. Drones kunnen personen ook gemakkelijk volgen. Bovendien zijn drones vaak niet of moeilijk zichtbaar, laat staan dat zichtbaar is dat daaraan een camera is bevestigd. Ook wordt de verantwoordelijke voor een extra uitdaging geplaatst om alle betrokkenen adequaat vooraf te informeren over het cameratoezicht.

Zoals eerder al is aangegeven, heeft de inzet van drones geen invloed op de wettelijke regelingen die in een concrete situatie van toepassing zijn. Relevante bepalingen van de Wbp en artikel 151c Gemeentewet j° de Wpg zijn uitgewerkt in de hoofdstukken 2, 3 en 4 van deze beleidsregels. Gelet op de eigenschappen en mogelijkheden van drones en de potentiële impact die drones kunnen maken op de persoonlijke levenssfeer van betrokkenen, zijn wel een aantal aandachtspunten te noemen.

Proportionaliteit en subsidiariteit

Allereerst is het van groot belang dat de verantwoordelijke zorgvuldig afweegt om al dan niet tot cameratoezicht door middel van drones over te gaan. De inzet van drones zal minder snel voldoen aan de eisen van proportionaliteit en subsidiariteit dan de inzet van statische camera's,[107] vanwege de mogelijkheid om drones (letterlijk en figuurlijk) flexibel in te zetten kan er ook meer inbreuk worden gemaakt op de persoonlijke levenssfeer van de betrokkenen. Het belang van het treffen van waarborgen ter bescherming van de persoonlijke levenssfeer wordt hierdoor bovendien onderstreept. Indien het doel van het cameratoezicht ook kan worden bereikt op een voor de burger minder ingrijpende wijze, bijvoorbeeld door middel van statische camera's, dan is de inzet van drones niet geoorloofd.[108]

Bovendien mag cameratoezicht op grond van artikel 151c Gemeentewet alleen betrekking hebben op openbare plaatsen (artikel 151c, lid 1 en 2, Gemeentewet). Het is dus niet toegestaan dat gemeenten ter handhaving van de openbare orde video-opnames maken van privévertrekken zoals tuinen en het interieur van woonhuizen.

Beveiliging

Een ander aandachtspunt is de beveiliging.[109] Sommige drones zijn uitgerust met de mogelijkheid om tijdens de vlucht camerabeelden te versturen naar het basisstation, alwaar ze kunnen worden uitgekeken. Hierbij bestaat het risico dat de beelden door onbevoegden 'uit de lucht' worden gehaald. Indien de camerabeelden op de drone of de daaraan verbonden apparatuur worden opgeslagen, bestaat het risico dat de beelden in handen van onbevoegden komen als de drone voortijdig uit de lucht komt vallen of uit de lucht wordt gehaald. De verantwoordelijke moet ook voor dergelijke situaties zorgen voor een adequate beveiliging, bijvoorbeeld door de camerabeelden te versleutelen met een deugdelijke encryptie.

Informatieplicht

Nog een aandachtspunt is het informeren van de betrokkenen.[110] In de regel geldt dat de betrokkenen moeten worden geïnformeerd dat er cameratoezicht plaatsvindt *alvorens* zij daadwerkelijk worden gefilmd. Dat kan in het geval van cameratoezicht door middel van drones problematisch zijn. Het is dan in ieder geval raadzaam om de betrokkenen via verschillende wegen te informeren. Te denken valt aan het plaatsen van borden aan de randen van het vlieggebied, een vooraankondiging en het verstrekken van actuele informatie op de website van de verantwoordelijke en via (sociale) media en bijvoorbeeld gemeentelijke nieuwsbrieven, het ter plekke uitdelen van informatiefolders en het zichtbaar en hoorbaar maken van de drones door middel van bijvoorbeeld felle kleuren, (knipperende) lichten en geluidssignalen.[111]
Indien de Wbp van toepassing is op het cameratoezicht, bestaat er een uitzondering op de informatieplicht. De informatieplicht geldt niet als het informeren van de betrokkenen onmogelijk blijkt of een onevenredige inspanning kost (artikel 34, lid 4, Wbp). Dit kan echter wel invloed hebben op de vraag of het cameratoezicht door middel van drones proportioneel is. Het niet kunnen informeren van de betrokkenen levert namelijk een grotere inbreuk op de persoonlijke levenssfeer van de betrokkenen. Die inbreuk kan daardoor disproportioneel worden in verhouding tot het met de verwerking te dienen doel.

---

[107] Zie over de vereisten van proportionaliteit en subsidiariteit paragraaf 2.7 en 3.7 'Noodzakelijkheid, proportionaliteit en subsidiariteit'.
[108] Zie ook *Kamerstukken II* 2012/13, 33 582, nr. 3, p. 12.
[109] Zie over het onderwerp beveiliging paragraaf 2.10 en 3.10 'Beveiliging'.
[110] Zie over de informatieplicht paragraaf 2.13 en 3.13 'Informeren betrokkenen'.
[111] Zie ook WP29, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, WP231, 16 juni 2015, p. 15–16.

Als het cameratoezicht plaatsvindt op grond van artikel 151c Gemeentewet, dan bestaat er *geen* uitzondering op de informatieplicht. De aanwezigheid van cameratoezicht op openbare plaatsen in het belang van de handhaving van de openbare orde moet altijd op een duidelijke wijze kenbaar zijn voor een ieder die de desbetreffende openbare plaatsen betreedt (artikel 151c, lid 6, Gemeentewet).

Voorbeeld drones geen persoonsgegeven
Een gemeente registreert door middel van een drone op welke wijze een mensenmassa zich verplaatst tijdens een evenement in het centrum van een stad. De camera filmt van dusdanige hoogte, zonder in te zoomen, dat de mensen niet herkenbaar in beeld worden gebracht. De mensen zijn ook anderszins niet identificeerbaar. Er is in dit geval geen sprake van een persoonsgegeven.

Voorbeeld drones persoonsgegevens
Een drone filmt de huizen in een woonwijk. De beelden van de huizen zullen meestal (indirect) tot personen te zijn herleiden. De drone-operator weet immers in principe waar de drone vliegt en opnames maakt (locatiegegevens). Vaak worden de locatiegegevens ook expliciet door de drone geregistreerd. Door middel van de camerabeelden en locatiegegevens is zonder onevenredige inspanning te achterhalen wie de eigenaars zijn van de betreffende huizen. Er is dan sprake van persoonsgegevens.

Voorbeeld drones ongerechtvaardigd
Een eigenaar van een fabriek controleert de binnenkant van de schoorstenen van de fabriek door middel van een camera die is bevestigd aan een drone. De camera maakt gedurende de gehele vlucht videoopnames. Hierdoor komen ook toeschouwers in beeld. Het is in dit geval voor het doel – controle van de schoorstenen – niet noodzakelijk dat gedurende de gehele vlucht video-opnames worden gemaakt. Volstaan kan worden om alleen video-opnames te maken op het moment dat de drone zich boven en in de schoorstenen bevond. Hierdoor kan worden voorkomen dat toeschouwers in beeld worden gebracht.

5.2 Dashcams

Een dashcam is een kleine videocamera, die speciaal gemaakt is om te filmen vanuit een auto. De dashcams zijn los verkrijgbaar of als inbouwapparatuur. De camera's kunnen automatisch beginnen met filmen zodra de auto gestart wordt, waardoor alle autoritten kunnen worden vastgelegd. In beginsel zijn alle dashcams hetzelfde: ze filmen de weg aan de voor- en/of achterkant van de auto. Er zijn een aantal opties die extra mogelijkheden aan de dashcam toevoegen, zoals een dashcam met een parkeermodus, met wifi[112] of GPS.[113]

Indien een dashcam personen in andere auto's herkenbaar filmt is de Wbp van toepassing. Ten aanzien van het filmen van kentekens geldt dat kentekens van motorvoertuigen persoonsgegevens zijn voor degenen die toegang hebben tot het kentekenregister van de Rijksdienst voor het Wegverkeer.[114] Onder de Wbp kan de verwerking van personen of een kenteken (indien een kenteken als persoonsgegeven gekwalificeerd kan worden) slechts gerechtvaardigd worden indien er een grondslag voor deze gegevensverwerking is (artikel 8 Wbp).

Voorbeeld toegestaan particulier gebruik dashcam
Dashcams worden vaak gebruikt bij verkeersongelukken. De dashcam kan met het beeldmateriaal van het verkeersongeluk zorgen voor het bewijs voor de verzekering. De gegevensverwerking van het beeldmateriaal van de dashcam kan noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang van de bestuurder (verantwoordelijke van de dashcam) om als bewijs te gebruiken voor zijn verzekering om zijn schade te declareren. Op basis van artikel 8 sub f Wbp kan het gerechtvaardigde belang hiervoor een grondslag bieden.

5.3 Slimme camera's

Andere slimme camera's – ook wel intelligente camera's genoemd – kunnen niet alleen 'waarnemen', maar ook informatie genereren. Een aantal voorbeelden van slimme camera's is:

- *Camera's met bewegingsdetectie:*
  Camera's met bewegingsdetectie slaan aan[115] zodra er beweging plaatsvindt. Ze worden in principe ingezet voor plaatsen waar normaliter geen beweging hoort te zijn. Een voorbeeld hiervan is een bedrijventerrein waar 's nachts geen bewegingen horen plaats te vinden.
- *Camera's met geluidsdetectie:*
  Camera's met geluidsdetectie slaan aan[116] zodra een bepaald geluidsniveau, type geluid of

[112] Om filmpjes of foto's eenvoudig naar de telefoon te downloaden.
[113] Een dashcam met GPS slaat de gereden routes op.
[114] *Kamerstukken II* 1998–1999, 25 892, nr. 6, p. 27.
[115] Dit kan inhouden dat de camera's continu opnemen, maar dat pas beelden worden getoond zodra beweging wordt geregistreerd, dan wel dat de camera's op het moment van beweging pas daadwerkelijk beginnen met opnemen.
[116] Ook hier geldt dat de camera's continu kunnen opnemen, maar dat pas beelden worden getoond zodra een bepaald geluid wordt geregistreerd, dan wel dat de camera's pas daadwerkelijk beginnen met opnemen op het moment van het geluid.

bepaalde woorden worden geregistreerd. Zo kan een camera noodkreten in diverse talen of gegil detecteren.

- *Camera's met gezichtsherkenning:*
  Camera's kunnen worden uitgevoerd met een techniek om gezichten te herkennen. Door middel van het koppelen van een gegevensbestand met gezichtskenmerken aan het camerasysteem kunnen personen op geautomatiseerde wijze worden geïdentificeerd.
- *Camera's met gedragsanalyse:*
  Camera's kunnen worden uitgevoerd met een techniek om diverse 'afwijkende' gedragingen te detecteren. Voorbeelden hiervan zijn detectie van iemand die een voorwerp ergens achterlaat en iemand die over een muur klimt.

Net zoals ten aanzien van drones, geldt ook hier dat de inzet van slimme camera's geen invloed heeft op de wettelijke regelingen die in een concrete situatie van toepassing zijn. Relevante bepalingen van de Wbp en artikel 151c Gemeentewet j° de Wpg zijn uitgewerkt in de hoofdstukken 2, 3 en 4 van deze beleidsregels. Hieronder volgt nog een aantal aandachtspunten die specifiek gelden voor slimme camera's.

Cameratoezicht door middel van slimme camera's kan tot gevolg hebben dat er een minder vergaande inbreuk op de persoonlijke levenssfeer wordt gemaakt dan door middel van 'reguliere' camera's.[117] Zo zullen de camerabeelden vaak pas worden bekeken wanneer de slimme camera's iets detecteren. De inbreuk op de persoonlijke levenssfeer wordt nog kleiner wanneer de slimme camera's pas beelden gaan *opnemen* zodra ze iets detecteren (dataminimalisatie).[118]

Aan de andere kant kan de inzet van slimme camera's juist ook tot gevolg hebben dat er sprake is van een grotere inbreuk op de persoonlijke levenssfeer. Camera's met gezichtsherkenning kunnen bijvoorbeeld personen op geautomatiseerde wijze traceren, volgen en profileren, hetgeen met reguliere camera's niet mogelijk is. Camera's die zijn uitgerust met een techniek voor gedragsanalyse, analyseren voorts de gedragingen van een ieder die in beeld komt. De gedragingen van die personen worden dus geanalyseerd zonder dat zij iets 'fout' hoeven te hebben gedaan. Bovendien hebben de camera's geen verstand en intuïtie, zodat gedragingen gemakkelijk verkeerd kunnen worden geïnterpreteerd.

Ten aanzien van camera's met gezichtsdetectie wordt nog het volgende opgemerkt. Dergelijke camera's identificeren personen aan de hand van gegevensbestanden met unieke gezichtskenmerken. Aangezien het op deze wijze dus mogelijk is om een persoon te identificeren, zijn ook de gezichtskenmerken in de bestanden persoonsgegevens in de zin van de Wbp. Voorts geldt dat verwerkingen door middel van dit soort camera's veelal identificatie tot doel heeft. Dit betekent dat de Autoriteit Persoonsgegevens de camerabeelden dan aanmerkt als rasgegevens in de zin van artikel 16 en 18 Wbp. De verwerking van rasgegevens is verboden behoudens de uitzonderingen die de Wbp noemt in artikel 17 tot en met 23.[119]

Voorbeeld slimme camera's geen gegevensverwerking
Een slimme camera telt hoeveel mensen er aanwezig zijn tijdens een evenement. De camera maakt geen video-opnames. Er is in dit geval geen sprake van een verwerking van persoonsgegevens.

Voorbeeld slimme camera's gerechtvaardigd
Een gemeente plaatst camera's met geluidsdetectie in een uitgaansgebied waar regelmatig opstootjes en vechtpartijen plaatsvinden (nadat andere maatregelen onvoldoende effectief zijn gebleken). Zodra de camera's geschreeuw, gegil of noodkreten detecteren, gaan ze beelden opnemen. De gemeente heeft de noodzaak van het cameratoezicht aangetoond. Bovendien leidt de inzet van de betreffende camera's tot dataminimalisatie ten opzichte van reguliere camera's, omdat niet continu beelden worden vastgelegd. De inzet van deze slimme camera's is in dit geval gerechtvaardigd.

Voorbeeld slimme camera's ongerechtvaardigd
Een theater wil een slimme camera ophangen bij de ingang van de theaterzaal om het aantal bezoekers te tellen. De camera telt automatisch het aantal bezoekers. Het is voor dit doel *niet* noodzakelijk dat de camera ook beelden opneemt. Het aantal bezoekers kan immers ook worden geteld zonder dat videoopnames worden gemaakt. Het aantal bezoekers mag dus wel worden geteld, maar het maken van de video-opnames is in dit geval niet gerechtvaardigd.

[117] Ervan uitgaande dat het gebruik van cameratoezicht voor dat doeleinde is toegestaan.
[118] Overigens hoeft er geen sprake te zijn van dataminimalisatie ingeval een camera pas beelden opneemt zodra er beweging plaatsvindt. Iedere beweging van een persoon wordt dan immers opgenomen.
[119] Zie over het onderwerp rasgegevens paragraaf 2.11 'Bijzondere persoonsgegevens' en paragraaf 3.11 'Gevoelige politiegegevens'.

6. Rechten van betrokkenen en rol van de Autoriteit Persoonsgegevens

Verantwoordelijken die in strijd handelen met de Wbp en de (Gemeentewet j°) Wpg kunnen op verschillende manieren in rechte worden aangesproken. Daarbij hebben betrokkenen een aantal mogelijkheden om zelf hun recht te halen en heeft de Autoriteit Persoonsgegevens als toezichthouder een aantal bestuursrechtelijke mogelijkheden om handhavend op te treden.

6.1 Rechten van betrokkenen[120]

De betrokkene die meent dat zijn persoonsgegevens onrechtmatig worden verwerkt, kan actie ondernemen door zijn klacht voor te leggen aan de verantwoordelijke.

Tevens heeft de betrokkene recht op inzage van de hem betreffende persoonsgegevens (artikel 35 Wbp en artikel 25 Wpg). Indien het cameratoezicht plaatsvindt op grond van artikel 151c Gemeentewet, moet het verzoek om inzage worden gericht aan de politie. Het recht op inzage is niet absoluut. Artikel 43 Wbp en artikel 27 Wpg noemen een aantal uitzonderingsgronden wanneer een verzoek tot inzage niet hoeft te worden gehonoreerd. Zo hoeft het verzoek niet te worden gehonoreerd wanneer dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten (artikel 43, sub b, Wbp) dan wel de goede uitvoering van de politietaak (artikel 27, lid 1, sub a, Wpg). Ook hoeft een verzoek niet te worden gehonoreerd wanneer dat noodzakelijk is in het belang van de bescherming van de betrokkene of van de rechten en vrijheden van anderen (artikel 43, sub e, Wbp en artikel 27, lid 1, sub b Wpg). Deze laatste uitzonderingsgrond betekent *niet* dat het verzoek mag worden afgewezen uitsluitend om administratieve lasten te beperken. Wél mag een verzoek worden afgewezen wanneer de verantwoordelijke aannemelijk kan maken dat zijn administratieve lasten zodanig disproportioneel zullen zijn dat hij in zijn rechten en vrijheden wordt aangetast of dreigt te worden aangetast.[121] De uitzonderingsgrond zal eerder van toepassing zijn wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is dan wanneer het verzoek is beperkt tot een bepaald(e) dag, tijdsperiode en locatie.

Naast het verzoek om inzage kan de betrokkene de verantwoordelijke verzoeken om zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt (artikel 36 Wbp en artikel 28 Wpg). Ten aanzien van cameratoezicht zal overigens eerder een verzoek tot verwijdering of afscherming aan de orde zijn, dan een verzoek om verbetering of aanvulling. Eveneens zal het verzoek er eerder op zien dat de camerabeelden niet ter zake dienend zijn voor de doeleinden van de verwerking, dan dat de beelden onjuist zijn. Indien het cameratoezicht plaatsvindt op grond van artikel 151c Gemeentewet, moet ook dit verzoek worden gericht aan de politie.

Indien de gegevensverwerking geschiedt op grond van de Wbp, kan de betrokkene bovendien onder bepaalde voorwaarden en in verband met bijzondere omstandigheden bij de verantwoordelijke verzet aantekenen. Als het verzet gerechtvaardigd is, moet de verantwoordelijke de verwerking beëindigen (artikel 40 Wbp).

Om de betrokkene te helpen bij het uitoefenen van zijn rechten, heeft de Autoriteit Persoonsgegevens een aantal voorbeeldbrieven op haar website gepubliceerd.[122]

Als een private organisatie of burger weigert te voldoen aan of niet reageert op het verzoek om inzage, het verzoek om verbetering, aanvulling, verwijdering of afscherming dan wel de aantekening van verzet, kan de betrokkene een verzoekschrift indienen bij de rechtbank (artikel 46 Wbp). Als de weigering of afwijzing geschiedt door een bestuursorgaan of de politie, dan zijn de bezwaar- en beroepsregels uit de Awb van toepassing (artikel 45 Wbp en artikel 29, lid 1, Wpg).

Voorts kan de betrokkene, indien een verantwoordelijke in strijd handelt met de Wbp, de rechter verzoeken om een verbod op te leggen op het verder verwerken van bepaalde persoonsgegevens (artikel 50 Wbp) of om hem een schadevergoeding toe te kennen (artikel 49 Wbp).

---

[120] Zie voor meer informatie over de rechten van betrokkenen de website van de Autoriteit Persoonsgegevens.
[121] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 171.
[122] Zie autoriteitpersoonsgegevens.nl

6.2 Onderzoek en handhaving door de Autoriteit Persoonsgegevens[123]

De Autoriteit Persoonsgegevens ziet toe op de naleving van de Wbp (artikel 51, lid 1, Wbp) en aanverwante wetten, waaronder de Wpg (artikel 35, lid 1, Wpg). Daartoe beschikt de Autoriteit Persoonsgegevens over een aantal middelen.

De Autoriteit Persoonsgegevens ontvangt signalen via de tipfunctie op autoriteitpersoonsgegevens.nl, het telefonisch spreekuur en per post. Het aantal aangedragen zaken en de complexiteit daarvan neemt echter voortdurend toe, terwijl de middelen die de Autoriteit Persoonsgegevens ter beschikking staan begrensd zijn. De Autoriteit Persoonsgegevens kan daarom niet alle zaken die worden aangebracht in behandeling nemen en moet keuzes maken. De Autoriteit Persoonsgegevens geeft prioriteit aan zaken waarbij zij een vermoeden heeft van ernstige, structurele overtredingen die veel mensen treffen en waarbij zij door de inzet van handhavingsinstrumenten effectief verschil kan maken of overtredingen die vallen binnen de (jaarlijkse) aandachtspunten die door de Autoriteit Persoonsgegevens bekend zijn gemaakt.[124]

De Autoriteit Persoonsgegevens kan signalen afhandelen door de verantwoordelijke die (mogelijk) een overtreding begaat hierop te wijzen in een (telefoon)gesprek of brief. Wanneer de verantwoordelijke de overtreding voorkomt of snel en correct beëindigt, kan de Autoriteit Persoonsgegevens volstaan met een waarschuwing en is geen nader onderzoek nodig.

Daarnaast kan de Autoriteit Persoonsgegevens een onderzoek instellen naar de naleving van de Wbp (artikel 60 Wbp) of de Wpg (artikel 35, lid 2, Wpg j° artikel 60 Wbp). Bij de uitvoering van een onderzoek kan de Autoriteit Persoonsgegevens haar toezichthoudende bevoegdheden inzetten, waarbij een verantwoordelijke verplicht is alle gevraagde medewerking te verlenen (artikel 5:20 Awb). De Autoriteit Persoonsgegevens kan onder meer inlichtingen vorderen (artikel 5:16 Awb), inzage vorderen in zakelijke gegevens (artikel 5:17 Awb), zaken en middelen onderzoeken, waaronder computerapparatuur (artikel 5:18 en 5:19 Awb), en ruimtes betreden, waaronder woningen (artikel 5:15 Awb en artikel 61, lid 2, Wbp).

Indien de Wbp of Wpg niet wordt nageleefd, kan de Autoriteit Persoonsgegevens bestuursdwang toepassen. Hiermee wordt bedoeld dat de Autoriteit Persoonsgegevens met feitelijk handelen kan optreden tegen een illegale situatie, doorgaans op kosten van de overtreder (artikel 65 Wbp en artikel 35, lid 2 Wpg j° artikel 5:21 Awb). Ook kan de Autoriteit Persoonsgegevens een last onder dwangsom opleggen (artikel 5:32 Awb). Een last onder dwangsom kan bijvoorbeeld inhouden dat een verantwoordelijke een gegevensverwerking moet aanpassen of staken binnen een vastgestelde termijn op straffe van een dwangsom van een bepaald geldbedrag per dag. Als de verantwoordelijke niet voldoet aan de last, kan het te betalen geldbedrag oplopen, tot een vooraf vastgesteld maximumbedrag.

Boetebeleidsregels Autoriteit Persoonsgegevens

Sinds 1 januari 2016 is de bevoegdheid van de Autoriteit Persoonsgegevens om een bestuurlijke boete op te leggen inzake overtredingen van onder meer de Wbp aanzienlijk uitgebreid.

De keuze van de wetgever om over te gaan tot uitbreiding van de boetebevoegdheid is ingegeven door de wens de sanctiemogelijkheden van de Autoriteit Persoonsgegevens te versterken om de naleving van de Wbp, zowel door bedrijven als overheden, te bevorderen.[125] Met de uitbreiding van de boetebevoegdheid van de Autoriteit Persoonsgegevens wordt toegegroeid naar het handhavingssysteem uit de toekomstige algemene verordening bescherming persoonsgegevens, die de Wbp als algemene wet zal gaan vervangen.[126] Ook het voorstel voor de verordening voorziet in de bevoegdheid voor de nationale toezichthouders om boetes op te leggen bij overtreding van de verordening.

De Autoriteit Persoonsgegevens heeft ervoor gekozen om in het kader van de uitbreiding van haar boetebevoegdheid boetebeleidsregels op te stellen die eveneens sinds januari 2016 van kracht zijn.

Met deze boetebeleidsregels beoogt de Autoriteit Persoonsgegevens inzicht te geven in hoe de hoogte van een bestuurlijke boete zal worden bepaald. Daarbij is uitgangspunt dat de hoogte van een boete evenredig moet zijn met het oog op de begane overtreding. In de boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte-systematiek: de beboetbare bepalingen op de naleving

[123] Zie voor meer informatie over het verrichten van onderzoek en het handhavend optreden door de Autoriteit Persoonsgegevens autoriteitpersoonsgegevens.nl
[124] Beleidsregels handhaving door het CBP van 31 januari 2011, *Stcrt.* 2011, 1916.
[125] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 4.
[126] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 11.

waarvan de Autoriteit Persoonsgegevens toezicht houdt, zijn per wettelijk boetemaximum van € 810.000, € 450.000 of € 20.250 ingedeeld in een aantal boetecategorieën met daaraan verbonden in zwaarte oplopende boetes. Daarnaast wordt inzicht gegeven in de relevante factoren die bepalend zijn voor de hoogte van een boete in het concrete geval.

BIJLAGE: RELEVANTE WETTELIJKE BEPALINGEN

Gemeentewet

Artikel 151c Gemeentewet (oud)

1. De raad kan bij verordening de burgemeester de bevoegdheid verlenen om, indien dat in het belang van de handhaving van de openbare orde noodzakelijk is, te besluiten tot plaatsing van vaste camera's voor een bepaalde duur ten behoeve van het toezicht op een openbare plaats als bedoeld in artikel 1 van de Wet openbare manifestaties en andere bij verordening aan te wijzen plaatsen die voor een ieder toegankelijk zijn. De burgemeester bepaalt de duur van de plaatsing en wijst de openbare plaats of plaatsen aan, met inachtneming van hetgeen daaromtrent in de verordening is bepaald.
2. De burgemeester stelt, na overleg met de officier van justitie in het overleg, bedoeld in artikel 13, eerste lid, van de Politiewet 2012, de periode vast waarin in het belang van de handhaving van de openbare orde daadwerkelijk gebruik van de camera's plaatsvindt en de met de camera's gemaakte beelden in elk geval rechtstreeks worden bekeken.
3. De burgemeester bedient zich bij de uitvoering van het in het eerste lid bedoelde besluit van de onder zijn gezag staande politie.
4. De aanwezigheid van camera's als bedoeld in het eerste lid is op duidelijke wijze kenbaar voor een ieder die de desbetreffende openbare plaats betreedt.
5. Met de camera's worden uitsluitend beelden gemaakt van een openbare plaats als bedoeld in artikel 1 van de Wet openbare manifestaties en andere bij verordening aan te wijzen plaatsen die voor een ieder toegankelijk zijn.
6. De met de camera's gemaakte beelden mogen in het belang van de handhaving van de openbare orde worden vastgelegd.
7. De verwerking van de gegevens, bedoeld in het zesde lid, is een verwerking als bedoeld in de Wet politiegegevens, met dien verstande dat, in afwijking van het bepaalde in artikel 8 van die wet, de vastgelegde beelden na ten hoogste vier weken worden vernietigd en de gegevens, bedoeld in het zesde lid, indien er concrete aanleiding bestaat te vermoeden dat die gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit, ten behoeve van de opsporing van dat strafbare feit kunnen worden verwerkt.
8. Bij of krachtens algemene maatregel van bestuur kunnen met het oog op de goede uitvoering van het toezicht, bedoeld in het eerste lid, regels worden gesteld omtrent:
   a. de vaste camera's en andere technische hulpmiddelen benodigd voor het toezicht, bedoeld in het eerste lid, en de wijze waarop deze hulpmiddelen worden aangebracht;
   b. de personen belast met of anderszins direct betrokken bij de uitvoering van het toezicht; en
   c. de ruimten waarin de waarneming of verwerking van door het toezicht vastgelegde beelden plaatsvindt.

Artikel 151c Gemeentewet (nieuw)

De Gemeentewet wordt gewijzigd als volgt:

Artikel 151c wordt gewijzigd als volgt:
1. In het eerste lid wordt de zinsnede 'te besluiten tot plaatsing van vaste camera's voor een bepaalde duur' vervangen door: te besluiten om voor een bepaalde duur camera's in te zetten.
2. De tweede volzin van het eerste lid vervalt.
3. Onder vernummering van het tweede en derde tot derde en vierde lid wordt na het eerste lid een nieuw lid ingevoegd, luidende: 2. De burgemeester besluit met inachtneming van het in de verordening van de raad bepaalde: a. binnen welk gebied, bestaande uit openbare plaatsen of andere voor een ieder toegankelijke plaatsen als bedoeld in het eerste lid, camera's worden ingezet; b. voor welke duur de gebiedsaanwijzing plaatsvindt.
4. Na het vierde lid (nieuw) wordt een lid ingevoegd, luidende:
5. De burgemeester trekt het besluit, bedoeld in het eerste lid, in zodra de inzet van camera's niet langer noodzakelijk is in het belang van de handhaving van de openbare orde.
5. Het vierde tot en met achtste lid (oud) worden vernummerd tot zesde tot en met tiende lid.
6. In het zesde lid (nieuw) wordt de zinsnede 'een ieder die de desbetreffende openbare plaats betreedt' vervangen door: een ieder die het gebied, bedoeld in het tweede lid, onder a, betreedt.
7. Het achtste lid (nieuw) komt te luiden:
8. Ten behoeve van de handhaving van de openbare orde worden in het kader van het toezicht, bedoeld in het eerste lid, gegevens verwerkt.
9. In het negende lid (nieuw) wordt de zinsnede 'bedoeld in het zesde lid' telkens vervangen door: 'bedoeld in het achtste lid'.
10. In het tiende lid, onder a, vervalt het woord: 'vaste'.

Wet politiegegevens

Artikel 1 – definities

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
a. *politiegegeven:* elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt;
b. *politietaak:* de taken, bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012;
c. *verwerken van politiegegevens:* elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens;
d. *verstrekken van politiegegevens:* het bekend maken of ter beschikking stellen van politiegegevens;
e. *ter beschikking stellen van politiegegevens:* het verstrekken van politiegegevens aan personen die overeenkomstig deze wet zijn geautoriseerd voor het verwerken van politiegegevens;
f. *verantwoordelijke:* dit is bij:
1°. de politie: de korpschef, bedoeld in artikel 27 van de Politiewet 2012;
2°. de rijksrecherche: het College van procureurs-generaal;
3°. de Koninklijke marechaussee: Onze Minister van Defensie;
4°. een gemeenschappelijke verwerking van politiegegevens met het oog op een gemeenschappelijk doel door twee of meer organisaties als bedoeld in dit onderdeel: de verantwoordelijke die door de betrokken verantwoordelijken is belast met de feitelijke zorg voor de verwerking en het treffen van de maatregelen, bedoeld in artikel 4;
g. *betrokkene:* degene op wie een politiegegeven betrekking heeft;
h. *het College bescherming persoonsgegevens:* het College, bedoeld in artikel 51 van de Wet bescherming persoonsgegevens;
i. *bewerker:* degene die ten behoeve van de verantwoordelijke politiegegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
j. *Onze Ministers:* Onze Ministers van Veiligheid en Justitie en van Defensie gezamenlijk;
k. *ambtenaar van politie:* de ambtenaar, bedoeld in artikel 2 van de Politiewet 2012, alsmede de ambtenaar van de Koninklijke marechaussee voor zover werkzaam ter uitvoering van de politietaken, bedoeld in artikel 4, eerste lid, van de Politiewet 2012, en, indien artikel 46 wordt toegepast, de ambtenaar, werkzaam bij de in dat artikel bedoelde dienst;
l. *gerelateerde gegevens:* de politiegegevens die bij de vergelijking van gegevens, bedoeld in de artikelen 8, tweede lid, 11, eerste en tweede lid, 12, vierde lid en 24, eerste lid, overeenkomen en de erbij behorende gegevens alsmede de politiegegevens waarmee bij het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8, derde lid en 11, vierde lid, verband blijkt te bestaan, voor zover verdere verwerking van de gegevens voor het betreffende doel noodzakelijk is;
m. *persoonsgegeven, ontvanger en toestemming van de betrokkene:* hetgeen daaronder wordt verstaan in de Wet bescherming persoonsgegevens;
n. *afschermen:* het markeren van opgeslagen politiegegevens met als doel de verwerking ervan in de toekomst te beperken;
o. *kenmerken* :het markeren van opgeslagen politiegegevens, zonder de bedoeling om hun toekomstige verwerking te beperken;
p. *bestand:* elk gestructureerd geheel van politiegegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Artikel 4 – juistheid, volledigheid en beveiliging politiegegevens

1. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij verbetert of vernietigt politiegegevens of vult deze aan indien hem blijkt dat deze onjuist of onvolledig zijn.
2. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.
3. De verantwoordelijke treft passende technische en organisatorische maatregelen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via directe geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's van de verwerking en de aard van de politiegegevens.

4. De verantwoordelijke heeft toegang tot de politiegegevens die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens deze wet bepaalde.
5. De verantwoordelijke verleent degenen die belast zijn met de controle en het toezicht, bedoeld in de artikelen 33, 34, 35 en 36, alsmede degenen die in zijn opdracht technische werkzaamheden verrichten toegang tot de politiegegevens die onder zijn beheer worden verwerkt, voor zover zij deze behoeven voor de uitvoering van hun taak.
6. De artikelen 14, eerste, tweede, derde en vijfde lid, 49 en 50 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.

Artikel 5 – gevoelige gegevens

De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

Artikel 25 – verzoek om kennisneming

1. De verantwoordelijke deelt een ieder op diens schriftelijke verzoek binnen zes weken mede of, en zo ja welke, deze persoon betreffende politiegegevens verwerking ondergaan. Hij verstrekt daarbij tevens desgevraagd inlichtingen over de vraag of de deze persoon betreffende politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt. De verantwoordelijke kan zijn beslissing voor ten hoogste vier weken verdagen, dan wel voor ten hoogste zes weken indien blijkt dat bij verschillende regionale of landelijke eenheden van de politie politiegegevens over de verzoeker worden verwerkt. Van de verdaging wordt schriftelijk mededeling gedaan.
2. Bij regeling van Onze Ministers kunnen nadere regels worden gesteld over het verzoek en de wijze van kennisneming.

Artikel 27 – uitzonderingen

1. Een verzoek, als bedoeld in artikel 25, eerste lid, wordt afgewezen voor zover het onthouden van kennisneming noodzakelijk is in het belang van:
   a. de goede uitvoering van de politietaak;
   b. de bescherming van de rechten van de betrokkene of van de rechten en vrijheden van derden;
   c. de veiligheid van de staat.
2. Een gehele of gedeeltelijke afwijzing vindt schriftelijk plaats.

Artikel 28 – verbetering, aanvulling, verwijdering, afscherming of markering van politiegegevens

1. Een ieder over wiens persoon politiegegevens worden verwerkt kan de verantwoordelijke schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.
2. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Artikel 37, eerste lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing. Een weigering is met redenen omkleed.
3. De verantwoordelijke draagt ervoor zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. Hij draagt zorg voor het kenmerken van een gegeven als de juistheid daarvan door de betrokkene wordt betwist en niet kan worden vastgesteld of het gegeven al dan niet juist is.

Artikel 29 – toepasselijkheid Awb

1. Een beslissing op een verzoek als bedoeld in artikel 25 of 28 geldt als een besluit in de zin van de Algemene wet bestuursrecht.
2. De artikelen 47 en 48 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.
3. In klachtprocedures waarbij de verantwoordelijke of onder zijn verantwoordelijkheid werkzame personen ingevolge artikel 9:31 van de Algemene wet bestuursrecht worden verplicht tot het verstrekken van inlichtingen of het overleggen van stukken aan de Nationale ombudsman met betrekking tot politiegegevens die zijn te herleiden tot een informant als bedoeld in artikel 12,

zevende lid, kan Onze Minister van Veiligheid en Justitie beslissen dat artikel 9:31, vijfde en zesde lid, van die wet buiten toepassing blijft.

4. Indien Onze Minister van Veiligheid en Justitie heeft beslist dat artikel 9:31, vijfde en zesde lid, van de Algemene wet bestuursrecht buiten toepassing blijft en de verantwoordelijke of onder zijn verantwoordelijkheid werkzame personen worden verplicht tot het overleggen van stukken, wordt volstaan met het ter inzage geven van de desbetreffende stukken. Van de desbetreffende stukken wordt op generlei wijze een afschrift vervaardigd.
5. In procedures inzake beslissingen als bedoeld in het eerste lid waarbij de verantwoordelijke of onder zijn verantwoordelijkheid werkzame personen ingevolge artikel 8:27, 8:28 of 8:45 van de Algemene wet bestuursrecht worden verplicht tot het verstrekken van inlichtingen of het overleggen van stukken met betrekking tot politiegegevens die zijn te herleiden tot een informant als bedoeld in artikel 12, zevende lid, kan Onze Minister van Veiligheid en Justitie beslissen dat artikel 8:29, derde tot en met vijfde lid, van die wet buiten toepassing blijft. Indien aan de rechtbank stukken dienen te worden overgelegd, wordt alsdan met het ter inzage geven van de desbetreffende stukken volstaan. Van de desbetreffende stukken wordt op generlei wijze een afschrift vervaardigd. Indien Onze Minister van Veiligheid en Justitie de rechtbank mededeelt dat uitsluitend zij kennis zal mogen nemen van de inlichtingen onderscheidenlijk de stukken, kan de rechtbank slechts met toestemming van de andere partijen mede op grondslag van die inlichtingen of stukken uitspraak doen.

Artikel 35 – toezicht Cbp

1. Het College bescherming persoonsgegevens ziet toe op de verwerking van politiegegevens overeenkomstig het bij en krachtens deze wet bepaalde.
2. De artikelen 51, tweede lid, 60, 61 en 65 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.
3. Indien de verantwoordelijke handelt in strijd met hetgeen is bepaald bij of krachtens artikel 32, kan het College hem een bestuurlijke boete opleggen. De artikelen 66 tot en met 74 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.
4. Het College bescherming persoonsgegevens wordt gehoord over de voorgenomen verwerking van politiegegevens, die in een nieuw bestand zullen worden opgenomen, wanneer deze verwerking de gegevens betreft, bedoeld in artikel 5, of wanneer de aard van de verwerking, in het bijzonder met gebruikmaking van nieuwe technologieën, mechanismen of procedures, specifieke risico's met zich meebrengt voor de fundamentele rechten van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer.

Wet bescherming persoonsgegevens

Artikel 1 – definities

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
e. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
f. betrokkene: degene op wie een persoonsgegeven betrekking heeft;
g. derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
h. ontvanger: degene aan wie de persoonsgegevens worden verstrekt;
i. toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;
j. Onze Minister: Onze Minister van Veiligheid en Justitie;
k. het College bescherming persoonsgegevens of het College: het College als bedoeld in artikel 51;
l. functionaris: de functionaris voor de gegevensbescherming als bedoeld in artikel 62;

m. voorafgaand onderzoek: een onderzoek als bedoeld in artikel 31;
n. verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;
o. verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens;
p. de Kaderwet: de Kaderwet zelfstandige bestuursorganen.

Artikel 8 – grondslagen voor verwerking

Persoonsgegevens mogen slechts worden verwerkt indien:
a. betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Artikel 10 – bewaartermijnen

1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

Artikel 16 – verwerking van bijzondere persoonsgegevens

De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Artikel 18 – rasgegevens

Het verbod om persoonsgegevens betreffende iemands ras te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt:
a. met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is;
b. met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen ten einde feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen en slechts indien:
   1°. dit voor dat doel noodzakelijk is;
   2°. de gegevens slechts betrekking hebben op het geboorteland van de betrokkene, van diens ouders of grootouders, dan wel op andere, bij wet vastgestelde criteria, op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een minderheidsgroep als bedoeld in de aanhef van onderdeel b behoort, en
   3°. de betrokkene daartegen geen schriftelijk bezwaar heeft gemaakt.

Artikel 33 – informatieplicht

1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens,

de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 34 – informatieplicht

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is:
   a. op het moment van vastlegging van hem betreffende gegevens, of
   b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.
5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

Artikel 34a [Treedt in werking per 01-01-2016]

1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.
5. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
6. Het tweede lid is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.
7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.
8. De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.
9. Dit artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.
10. Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.
11. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.

Artikel 35 – inzagerecht

1. De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden

verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.
2. Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.
3. Voordat een verantwoordelijke een mededeling doet als bedoeld in het eerste lid, waartegen een derde naar verwachting bedenkingen zal hebben, stelt hij die derde in de gelegenheid zijn zienswijze naar voren te brengen indien de mededeling gegevens bevat die hem betreffen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.
4. Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.

Vrijstellingsbesluit Wet bescherming persoonsgegevens

Artikel 38 – Videocameratoezicht

1. Artikel 27 van de wet is niet van toepassing op verwerkingen met het oog op de beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen, die zijn toevertrouwd aan de zorg van de verantwoordelijke, door middel van het gebruik van duidelijk zichtbare videocamera's, voor zover deze verwerkingen voldoen aan de in dit artikel vermelde eisen.
2. Het eerste lid is niet van toepassing op verwerkingen met het oog op de handhaving van de openbare orde.
3. De verwerking geschiedt slechts voor:
   a. de bescherming van de veiligheid en gezondheid van een of meer natuurlijke personen;
   b. de beveiliging van de toegang tot gebouwen en terreinen;
   c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
   d. de controle op een productieproces;
   e. het vastleggen van incidenten.
4. Geen andere persoonsgegevens worden verwerkt dan:
   a. video-opnamen van de gebouwen en terreinen en zich daarop bevindende personen en zaken, waarover de zorg van de verantwoordelijke zich uitstrekt;
   b. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.
5. De persoonsgegevens worden slechts verstrekt aan:
   a. degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de in het derde lid bedoelde activiteiten of die daarbij noodzakelijk zijn betrokken;
   b. ambtenaren van de politie in geval van incidenten, ingevolge artikel 8, onder e, van de wet;
   c. anderen, in de gevallen bedoeld in artikel 8, onder a, c en d, en artikel 9, derde lid, van de wet.
6. De persoonsgegevens worden verwijderd uiterlijk vier weken nadat de opnamen zijn gemaakt, dan wel na afhandeling van de geconstateerde incidenten.

Contactgegevens

Bezoekadres

(alleen volgens afspraak)
Prins Clauslaan 60
2595 AJ DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres

Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer 0900-2001 201. De publieksvoorlichters zijn bereikbaar op werkdagen van 09.30 tot 12.30 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting

Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer 070-8888 555.

Zakelijke relaties

Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer 070-8888500